PhD-FSTM-2025-025

The Faculty of Science, Technology and Medicine

DISSERTATION

Presented on 14/02/2025 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Alexandre AMARD

Born on 3 October 1987 in Mont-Saint-Martin (France)

DELIVERING HUMAN-CENTERED DIGITAL PUBLIC INFRASTRUCTURE – A PUBLIC VALUES AND GOVERNANCE ANALYSIS OF DIGITAL IDENTITIES

Dissertation defence committee

Dr. Gilbert Fridgen, Dissertation Supervisor
Full Professor, Université du Luxembourg

Dr. Andreas Hein, Chairman
Associate Professor, Université du Luxembourg

Dr. Nils Urbach, Vice-Chairman
Professor, Frankfurt University of Applied Sciences

Dr. Liudmila Zavolokina
Assistant Professor, University of Lausanne

Dr. Andreas Braun
Director, Artificial Intelligence Lab, PwC

Acknowledgements

I extend my heartfelt gratitude to my thesis supervisor, Prof. Gilbert Fridgen, for his enthusiasm for this research stream, his unwavering support, and his invaluable guidance throughout our collaboration.

I am equally grateful to my thesis supervision committee (CET), Prof. State and Prof. Urbach, for their insightful and benevolent guidance, which has been tremendously valuable, and to my Jury Members, Prof. Zavolokina, Dr. Braun and Prof. Hein, for challenging me to achieve the highest standards in my scientific work.

I thank the Luxembourg National Research Fund (FNR) and PayPal (Grant agreement P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen) for their funding, which made this research possible. For the purpose of open access and in fulfillment of the obligations arising from this grant agreement, I have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

I also want to thank my co-authors and colleagues who have joined me on this academic journey. This has been as much a human adventure as it has been a professional one, and each of you have contributed in meaningful ways.

This research would have been impossible without the community of incredibly talented researchers and practitioners active on these fundamental topics that impact so many lives. The exceptional work being performed daily in this community is humbling, and a very particular thanks naturally goes to all the interview partners that took part in this research, and the inspiring figures of this community who have guided my steps. I dedicate this thesis to them.

Lastly, my deepest gratitude goes to my family and friends, who have always been there for me, and who are the most precious thing in this life.

Abstract

In 2021, an estimated 850m people around the world were lacking means of identification, challenging the United Nations' Sustainable Development Goal 16.9, legal identity for all, including birth registration, by 2030. Digital identity infrastructure is increasingly considered as a means to tackle this challenge and effectively enable society-wide functions and services. The development of reliable digital identity infrastructure has become a high priority for governments to enable their citizens to take full advantage of the opportunities that digitalization represents. At the same time, critical researchers have uncovered that inadequately designed government-led digital infrastructure often leads to negative societal outcomes, by failing to uphold public values such as inclusion, citizen protection and sustainability. This cumulative thesis investigates how digital identity infrastructure design interrelates with a public values approach, proposing an analytical lens to concisely apprehend governance and institutional design decisions to deliver human-centric outcomes. It does so using qualitative methods borrowed from the information systems and political science domains. It proposes a refined public values framework fit for our new reality of digital public infrastructure deployment, and a taxonomy of strategic governance and institutional decisions when designing digital identity infrastructure. These tools can be used by both researchers and practitioners to guide digital identity infrastructure design and evaluation, and this dissertation concludes with an instantiation thereof. Collectively, these contributions build a foundation for the contextualization of digital infrastructure development with a human-centric perspective.

Table of contents

Acronyms

CAG	Comptroller and Auditor General of India
DEG	Digital Era Governance
DPGA	Digital Public Goods Alliance
G20	Group of Twenty
GiZ	Deutsche Gesellschaft für Internationale Zusammenarbeit, *German International Cooperation Society*
HIC	High-Income Countries
ID4D	Identification for Development
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LMIC	Low- and Medium-Income Countries
MOSIP	Modular Open Source Identity Platform
NCRA	National Civil Registration Authority (Sierra Leone)
NPM	New Public Management
OECD	Organisation for Economic Co-operation and Development
ONECI	Office National de l'Etat Civil et de l'Identification (Guinea)
PVM	Public Value Management
UNDP	United Nations Development Programme
UNHCR	United Nations High Commissioner for Refugees
USAID	United States Agency for International Development

List of Tables

I | Introduction

1 Why research Digital Identity Governance?

In 2021, approximately 850 million individuals worldwide lacked access to any form of identification, posing a significant challenge to the United Nations' Sustainable Development Goal 16.9, which aims to achieve legal identity for all, including birth registration, by 2030 (World Bank, 2021). Beyond this, a substantial portion of those with identification means face barriers to utilizing it online, exacerbating digital exclusion (Hundal & Chaudhuri, 2020; Ranchordas, 2020; Tavares & Masiero, 2023; Watling, 2011). This gap not only creates inequalities in opportunity but also prevents individuals from accessing essential services such as direct cash transfers or government subsidies, which increasingly rely on digital platforms for efficient distribution.

Global efforts to implement remote identification systems are gaining momentum (RP3). These initiatives aim to build national capacity to enable citizens to securely identify and authenticate themselves remotely. For instance, India's Aadhaar system has incorporated features that allow remote biometric verification for service access, while Estonia's e-Residency program offers a digital identity solution enabling secure cross-border authentication. By facilitating distance-based identification, such systems lay the groundwork for more inclusive service delivery, particularly in sectors like healthcare, social protection, and financial inclusion (Gelb & Diofasi, 2018).

These systems, however, frequently encounter significant challenges that lead to failure, either by falling short of delivering the anticipated capabilities or, in more insidious ways, by generating adverse outcomes that perpetuate the very inequalities and exclusion they were designed to address (Heeks, 2002; Inuwa et al., 2019; Masiero & Arvidsson, 2021). Such failures are often attributable to governance or institutional shortcomings in the design and implementation of the infrastructure.

The critical importance of getting digital identity systems right cannot be overstated. As digital identity becomes increasingly integrated into daily life, virtually every individual worldwide will become dependent on such systems for their livelihood. Failure to design and govern them effectively risks causing irreparable harm, triggering cascades of exclusion, and denying access to vital, life-changing services. Ensuring that these systems are appropriately designed and governed is essential for their success and their ability to drive societal progress.

Research on digital identity infrastructure governance remains limited within the academic literature. While some scholars have explored digital identity beyond purely technical considerations, contributing valuable and insightful work that highlights its significance, much of this research has primarily taken a descriptive and critical approach. What remains largely absent is an information systems engineering perspective that addresses the structural and functional aspects of digital identity governance in a systematic manner. This gap underscores the need for further exploration and theoretical development in this area to support more comprehensive and actionable insights.

2 Research Aim

Accordingly, this thesis aims to contribute to the global body of research by providing actionable insights that support both theoretical development and the practical implementation of digital identity infrastructure that achieves its intended outcomes. Through a combination of scientific publications, this cumulative thesis aims to bridge the divide between theoretical advancements and practical implementation, providing actionable frameworks and insights to guide the development of effective, inclusive, and sustainable digital identity systems.

Central to this research is the recognition that digital identity systems must prioritize the needs, rights, and lived experiences of individuals who rely on them (Anand & Brass, 2021; Beduschi, 2021; Rahaman & Sasse, 2010). By placing human-centricity at the forefront, this thesis seeks to identify ways in which service designers and policymakers can create digital identity infrastructure that not only functions effectively but also fosters the upholding of public values such as trust, inclusion and sustainability.

Equally important is understanding the role of governance and institutional design in ensuring the long-term success of digital identity systems. Governance frameworks shape how these systems are developed, operated, and maintained. This in turn influences their sustainability, and acceptance by stakeholders (Manoharan et al., 2023). Institutional arrangements, including the roles of public and private actors, regulatory frameworks, and accountability mechanisms, play a pivotal role in determining the infrastructure’s impact and resilience (Manoharan et al., 2023; Yang et al., 2024). This thesis aims to analyze these dimensions, offering practical recommendations to design governance structures and institutional alignment with the intended objectives of digital identity systems.

To address these aims, this research investigates two key questions: (1) What governance options are available to service designers and policymakers in the design of digital identity infrastructure? and (2) How can digital identity governance and institutional design support the creation of systems that uphold public values? By answering these questions, this thesis aspires to advance theoretical understanding and offer actionable guidance for stakeholders engaged in the development and implementation of digital identity systems. This dual focus on supporting theory-building and practical application ensures that the findings are both academically valuable and directly applicable to real-world challenges.

3 Structure

This cumulative thesis is structured in five sections. Section II provides a conceptual background on the primary concepts explored in this thesis: public values and its relation to human-centeredness, and digital identity infrastructure as one type of digital public infrastructure. It is based on six research papers (RP1; RP2; RP3; RP4; RP5; RP6) and one book chapter (BC1) and answers the first research question of this thesis. After these foundational bases have been established, section III juxtaposes these concepts by proposing an analytical lens of the digital identity governance framework developed in (RP1; RP2) with considerations for human-centeredness uncovered in (RP4; RP5), answering research question 2.

Finally, section IV concludes this thesis with a summary of its research contributions, a discussion of the limitations of each individual study, and outlines directions for future research.

Domain	Publication	Title	Outlet	Ranking	Role
Digital identity infrastructure governance	RP #01	Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices	Hawaii International Conference on System Sciences (HICSS)	GGS Class: 2 GGS Rating: A	Single Primary Author
	RP #02	Challenges in designing digital identity infrastructure for development: A taxonomy of strategic institutional and governance choices	Information Technology for Development (IT4D) (under review)	Scopus: 97%	Single Primary Author
	RP #03	The EU's Digital Identity Policy: Tracing Policy Punctuations	United Nations University's International Conference on Theory and Practice of Electronic Governance (ICEGOV)	GGS Class: WIP GGS Rating: WIP	Joint Primary Author
	BC #01	Decentralized Digital Identities	Decentralization Technologies in Finance	N/A	Joint Primary Author
Human-centeredness in eGovernment	RP #04	User-centricity and Public Values in eGovernment: Friend or Foe?	European Conference on Information Systems (ECIS)	GGS Class: 2 GGS Rating: B	Non-Primary Author
	RP #05	When Public Values and User-Centricity in eGovernment Collide – a Systematic Review	Government Information Quarterly (GIQ)	Scopus: 99%	Joint Primary Author
	RP #06	Guiding Refugees Through European Bureaucracy: Designing a Trustworthy Mobile App for Document Management	The Transdisciplinary Reach of Design Science Research (DESRIST)	GGS Class: WIP GGS Rating: WIP	Joint Primary Author

RP: Research Paper | BC: Book Chapter

Table 1: Publications overview.

II | Public Values and Human-Centeredness in Digital Public Service Delivery

1 Public values in eGovernment

“Public values” refer to the principles and norms that guide public institutions and services in achieving the common good (RP1; RP2). Rooted in public administration theory, the concept of public values has been explored extensively by scholars seeking to define and operationalize the ethical and practical priorities of governance and service delivery (Bozeman, 2007; Jørgensen & Bozeman, 2007). They can be defined as “a mode of behavior [or] a way of doing things […] that is held to be right […] by the public, citizens or the so-called ‘reasonable man’” (Bannister & Connolly, 2014). In government, public values are those that provide “normative consensus about (a) the rights, benefits, and prerogatives to which citizens should (and should not) be entitled; (b) the obligations of citizens to society, the state, and one another; and (c) the principles on which governments and policies should be based” (Frederickson, 1990; Jørgensen & Bozeman, 2007; Nabatchi, 2012).

Public values encompass a range of ideals, including equity, accountability, transparency, efficiency, and sustainability. These values are dynamic, evolving in response to societal changes, technological advancements, and shifting public expectations (Bryson et al., 2014). While human-centeredness focuses on the design and delivery of services, public values provide the ethical and normative framework that guides their development. Together, they ensure that public systems are not only functional but also aligned with societal priorities and expectations.

Public values evolve with time and with the societies that generate them. This makes them not exact science but very much human. Still, many researchers have attempted to inventorize them, using different methods. Recent research examining the state of the literature on public values compiles upwards of 30 public values, categorized in three types: duty-oriented, service-oriented and socially-oriented (RP4; RP5). An important takeaway of these renewed stock-taking exercises is that values morph with the circumstances of the times, and that similar values are expressed with different words and nuances, adding to their complexity (RP5; Bannister & Connolly, 2014; Jørgensen & Bozeman, 2007).

DUTY-ORIENTED	SERVICE-ORIENTED	SOCIALLY ORIENTED
Responsibility to the citizen / political neutrality	Service to the citizen in his or her different roles	Inclusiveness
Compliance with the law	Respect for the individual	Justice
Efficient use of public funds	Responsiveness / proactivity / flexible service delivery	Fairness / equity
Facilitating the democratic will	Effectiveness	Equality of treatment and access
Accountability to government	Efficiency	Respect for the citizen
Economy of public funds	Transparency	Due process
Rectitude	Productivity	Protecting citizen privacy
Legitimacy	Innovation	Protecting citizens from exploitation
Representation of citizens' will and needs		Protecting citizen security
Sustainability		Accountability to the public
		Consultation / participation / engagement
		Impartiality
		Pluralism / diversity
		Trust / confidence / reliability

Table 2: Framework of Public Values (RP4; RP5).

Public values should also be apprehended with the understanding of their multiplicity, and the fact that they are often congruent or contrasting with each other. Recent research has explored the idea of public values pluralism, and their intrinsic multiplicity and hybridity (van der Wal & van Hout, 2009). Behind this idea is that public values cannot be reduced to a unitary conception. Rather, conflict is prevalent, both internally and in relation to each other (RP5; Jørgensen & Bozeman, 2007). Researchers have explored many examples over the years, such as the fact that public values of governing with integrity (e.g., transparency, fairness, rectitude) and governing effectively/efficiently can conflict (RP4; RP5; De Graaf et al., 2016; de Graaf & van der Wal, 2010).

Another challenge is that not only do certain public values conflict between each other, but user-centric principles often conflict with certain public values as well (e.g., user involvement and accountability, user focus and pluralism) (RP4; RP5). While further investigation is needed to determine the theoretical implications of these conflicts, research has started to unravel the sources of conflict and conflict dimensions in an e-government context, establishing the bases to build a theoretical frame and propose recommendations to policy-makers on ways to avoid or mitigate these conflicts (RP5).

2 Human-centeredness as a method to embed public values in public service delivery

Despite the conflicts between public values, approaches to uphold them as part of public service delivery have blossomed, driven by a desire to develop services that are not only appropriate, but also beneficial, to humankind. Human-centeredness originates from human-centered design, which emerged in the mid-20th century as a response to the growing complexity of technological systems and their interaction with users. Central to human-centered design is the belief that systems, services, and technologies should be designed with a deep understanding of human needs, preferences, and behaviors (Norman, 1988). The approach emphasizes empathy and iterative processes to create solutions that are not only functional but also accessible, inclusive, and meaningful to users.

The principles of human-centeredness have been applied across various fields, including organizational management, healthcare, and public services (Carayon et al., 2020; Junginger, 2017). In each context, the core tenets remain consistent: a focus on usability and accessibility, and a commitment to addressing the emotional and experiential aspects of the user experience (Krippendorff, 2005). These principles aim to ensure that solutions are not just effective but also desirable, fostering a sense of ownership and trust among end-users.

In the public sector, human-centeredness has evolved into a broader philosophy that influences service delivery, policymaking, and organizational design. It has been recognized as a critical factor in addressing systemic inequities and improving citizen engagement (Holeman & Kane, 2020; Nihei, 2022). Scholars have argued that a human-centered approach in public services can lead to more inclusive and adapted systems, particularly in addressing the needs of underserved and marginalized populations (Bason, 2017; Jones, 2016; Walton, 2016). In essence, human-centered design is useful to transform abstract public values into tangible outcomes, bridging the gap between citizen expectations and institutional practices (Niemelä & Melkas, 2019; Røhnebæk et al., 2019). This is one of its primary distinctions from another service design approach, user-centered design. While user-centered design focuses primarily on the ability of a user to effectively interact with a specific system or interface, human-centered design considers the broader context of human needs, behaviors, and societal impact (Gasson, 2003; *ISO 9241-210*, 2019). In fact, while user-centricity and public values can often conflict (RP5), human-centricity and public values are by definition symbiotic.

In developing countries, digitalization is increasingly recognized as a potential solution to pressing challenges such as poverty and limited access to essential services and economic opportunities (Inoue, 2024; Mothobi & Grzybowski, 2017; Spulbar et al., 2022). However, the development of digital systems is constrained by limited financial resources and expertise, which hampers the emergence of a robust, iterative, and competitive ecosystem capable of addressing these urgent needs. Consequently, siloed, non-synergistic implementation projects—often delivered by single vendors—have become the norm. Despite the frequent failure of such projects to uphold public values, the significant imbalance between the implementers of digital services and the populations they serve leaves little room for redress or recourse (Tavares & Masiero, 2023). This disparity is further intensified by the affected populations' limited capacity to comprehend the complex systems and dynamics that drive these failures and injustices (Chaudhuri, 2021).

In response to these challenges, human-centered approaches are now seen as a vital strategy for addressing digital infrastructure needs in developing countries.

3 Digital Public Infrastructure

With this growing emphasis on upholding public values, researchers and governments have steadily pursued innovative approaches to enhance public service delivery. This evolving focus is reflected in the development of various paradigms within public administration. For instance, the New Public Management (NPM) approach, prominent in the late 20th century, advocated adopting private-sector practices to enhance efficiency and outcomes in public service delivery, framing users as customers (Bryson et al., 2014; Walker et al., 2011). While NPM aimed to introduce market-oriented reforms, its emphasis on efficiency often overlooked broader public values such as equity and inclusivity.

In response, the early 2000s saw the emergence of the Public Value Management (PVM) paradigm, which shifted focus from market-based solutions to collaboration and citizen engagement (Bryson et al., 2014). This approach emphasized the co-creation of solutions, positioning citizens as active participants in governance rather than passive recipients of services (Stoker, 2006). PVM underscored the importance of addressing societal needs collectively, fostering accountability, and enhancing trust between governments and their constituents.

With the rise of digitalization, these frameworks have been further refined through the Digital Era Governance (DEG) approach (Dunleavy, 2005). DEG emphasizes the re-aggregation of services to reduce fragmentation, promotes citizen-centric design to better align services with user needs, and leverages digital technologies to streamline processes and improve accessibility (Dunleavy et al., 2006).

Together, the evolution of these paradigms illustrates the ongoing evolution of public administration in its pursuit of more effective, inclusive, and value-driven service delivery. Digital Public Infrastructure emerged within this trajectory as a tangible embodiment of public values, offering concrete implementation principles that reflect these ideals. Digital Public Infrastructure is considered as foundational, interoperable shared digital systems that promote access to digital services for all (G20, 2023; UNDP, 2023). As an implementation method, and unlike approaches that emphasize methods (e.g., citizen participation), Digital Public Infrastructure focuses on achieving desired outcomes, such as efficiency, inclusivity, and accessibility. Fundamentally, it recognizes that the digital delivery of public services demands a foundational system that integrates the structural rigor of an infrastructural model with a commitment to the ethos of public values. This dual focus aims to ensure that the infrastructure not only supports effective service delivery but also reinforces the ethical and societal priorities central to governance.

However, intent does not guarantee outcomes, and public infrastructure is also subject to challenges when it comes to delivering its desired societal benefits. For example, more and more public infrastructure is partially privately owned, making the upholding of public values challenging (Koppenjan et al., 2008). As a response, practitioners and academics have called for the safeguarding of public values by contracts, regulation, and oversight structures (Bruijn & Dicke, 2006).

4 Digital Identity Infrastructure Governance

Digital identity infrastructures can be defined as systems that construct, control, and commodify (facets of) digital identities and can be formed by both public and private sector actors (Giannopoulou, 2023). They are an operationalization of digital infrastructure, i.e., digital, socio-technical systems that underlie or support the public interest, as well as universal or quasi-universal services (Plantin et al., 2018).

Digital identity infrastructure is increasingly considered as a means to support sustainable development, and effectively enable society-wide functions and services provided by the government or private sector (DPGA & GiZ, 2022; Gelb & Diofasi, 2018; Henfridsson & Bygstad, 2013). The benefits commonly associated with digital identity infrastructure are multiple, and particularly transformative in low- and middle-income countries (LMICs). Both academics and practitioners have highlighted its capacity to support socio-economic development, enable individual agency and improve inclusion.

In light of these asserted benefits, the development of reliable digital identity infrastructure has become a high priority for governments to enable their citizens to take full advantage of the opportunities that digitalization represents (Gelb & Diofasi, 2018), and a number of countries around the world have built their own digital identity capabilities, including India, Nigeria, Ethiopia, Peru and the Philippines. Many more commit substantial resources to build or improve their own digital identity infrastructures (World Bank, 2022).

Digital identity infrastructures incorporate the reality of interconnected system collectives, which evolve at the intersection between socio-technical elements, networks of actors and relationships between organized practices (Henfridsson & Bygstad, 2013). They are thus structured by complex socio-technical systems (van Dijck & Jacobs, 2020; Weigl, Barbereau, Rieger, et al., 2022b). Organizational and institutional arrangements significantly influence the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), thus playing an important role in the design of digital identity infrastructure. It follows that considering actors, roles, people and processes is a necessary condition for the development and implementation of useful and sustainable infrastructures (Dawes, 2009; Manny et al., 2022). Digital identity infrastructure design and success are therefore inextricably interlocked with the strategic governance choices that impact them (Gil-Garcia & Flores-Zúñiga, 2020; Medaglia et al., 2022), and their identification and characterization should be a priority.

A detailed look at instantiations around the world reveals wildly different implementations and substantial design complexity. For example, in Scandinavian countries, banks play a crucial role in providing digital identity services to citizens who use their 'BankID' on a daily basis for various identification purposes (Husz, 2018). On the other hand, the Indian Aadhaar system is led by the public sector, with extensive participation of the private sector, including for the enrolment of citizens (UIDAI, 2023). On the other side of the spectrum, Bhutan recently adopted a bill establishing a digital wallet enabling its citizens to assert control on the disclosure of their identity data during identification and authentication transactions (Parliament of Bhutan, 2023). These are just a few of the existing governance configurations in an area where disruptive technologies are increasingly deployed.

Faced with this complexity, and in response to the impact of these governance and institutional arrangements on the design and ultimate success of the costly infrastructure, frameworks have been developed to list and classify the strategic choices that service designers and policy makers are faced with when developing digital identity infrastructure (RP1; RP2).

The taxonomy for strategic institutional and governance choices for digital identity infrastructure (Table 3, RP2) in particular has proven its usefulness in both research and practical contexts, having been used as analytical framework in adjacent domains (Degen & Teubner, 2024) and in digital identity infrastructure institutional design in a West African country. Centered around four dimensions: institutional arrangement, ecosystem management, funding management and data management, it outlines the many dimensions that compose institutional and governance decisions for digital identity in governmental contexts.

	Layer	Dimension	Characteristics				
Strategic Institutional and Governance Choices for Digital Identity Infrastructure	Institutional Arrangement	**Authority governance model** *(mutually exclusive)*	Inter-ministerial entity	Ministerial entity	Semi-autonomous entity (with stakeholder representation)	Fully autonomous entity (with direct Cabinet- or Executive-level reporting)	
		Additional authority prerogatives	Civil registration	Identity document and certificates issuance	Others (e.g. statistics, digitalization strategy)	Single purpose authority	
	Ecosystem Management	**Subjects**	Nationals (residents)	Nationals (non-residents)	Non-nationals (residents)	Non-nationals (non-residents)	Persons without proof of legal identity
		Geographical scope	Sub-national	National	Transnational		
		Interoperability approach	None	Mutual recognition	Harmonization		
		Interoperability enablers	Standards (technical, organizational, semantic)	Certification or accreditation mechanisms	Open-source / community software		
		Roles of private sector actors	None	Identity consumption	Identity provision	Registrar	Infrastructural provision
	Funding Management	**Development funding**	Public funding	Public-private partnership	Grant		
		Operational financing	Public budget	Charge for relying parties	Charge for data subjects	Other	
	Data Management	**Data presentation model**	Identity provider to relying party	Federation through 1 actor	Federation through multiple actors	Data subject to relying party	
		Identity matching approach	Mediated	Non-mediated			
		Trusted sources	Government-controlled databases	Digital wallets	Distributed ledgers		

Table 3: Taxonomy of strategic institutional and governance choices for digital identity infrastructures (RP2).

III | Public Values in Digital Identity Governance

Against this backdrop and drawing on the theoretical and practical resources presented in the publications comprising this thesis, this section develops an instantiation of the taxonomy proposed by (RP2), examined from the perspective of public values as refined in (RP4; RP5). Fundamentally, it synthesizes the key concepts developed throughout the thesis and addresses the second research question originally posed (how can digital identity governance and institutional design support the creation of systems that uphold public values?).

This instantiation also demonstrates how the individual contributions of this thesis can help uncover the relationship between institutional and governance choices and the realization of a digital identity infrastructure's expected outcomes. To achieve this, a subset of analytical considerations can be selected, prioritizing those most relevant to the actualization of benefits as identified in both scientific and grey literature. While incorporating additional considerations could provide valuable qualitative insights, the necessary limitation in scope means that the selected examples should be viewed as illustrative rather than exhaustive.

Actualization of the benefits linked to digital identity infrastructure requires its adoption by citizens and service providers, and its usage over time. The societal value of digital infrastructure is not intrinsic: it relies on the affordances it enables and the services that leverage it in a specific organizational context (Kumar, 2004). However, negative impacts on the actualization of public values can be generated from the very design of digital public infrastructure. Bannister & Connolly (2014) propose that information and communications technology has the potential to cause highly negative impact on *inclusion* (i.e., social inclusion and equality of treatment and access) and *citizen protection* (in particular through a privacy lens). This is corroborated by the focus on these two considerations of both academic research (see, among others, Addo & Senyo, 2021; Anand & Brass, 2021; Beduschi, 2021; Chudnovsky & Peeters, 2021; Giannopoulou, 2020; Martin & Taylor, 2021; Masiero, 2018; Masiero & Arvidsson, 2021; Mir et al., 2019; Park & Humphry, 2019; Tavares & Masiero, 2023; Wang & Filippi, 2020; Wickins, 2007) and grey literature (see 50-in-5, 2023; ITU, 2018; McKinsey, 2019; OECD, 2023; UNHCR, 2018; USAID, 2017; World Bank, 2023b). *Citizen protection* in turn influences citizens' perceived risk, which when coupled with *trust*, act as clear determinants to adoption of governmental digital identity solutions (Bélanger & Carter, 2008; Hooda et al., 2022; Kubicek & Noack, 2010b; Li et al., 2008), a position shared by practitioners (European Commission, 2021a; ITU, 2018; OECD, 2023). Finally, the infrastructures' *sustainability*, and its resilience over time, directly impacts the duration for which these benefits can be realized (Bocchini et al., 2014) and is thus an important factor in effectiveness considerations in particular in LMICs (Gurara et al., 2018). In light of their characteristics, these four considerations can be considered as pre-requisites for the actualization of benefits linked to digital identity. Anand & Brass (2021) uses the term 'design imperatives' to refer to these considerations, while the World Bank's ID4D program (2022) uses the term 'principles'. A better understanding of how governance decisions can impact them is therefore critical.

The analysis in the following section draws on academic and grey literature, as well as archival records. It uncovers examples of anticipated impacts that decisions within each dimension of the taxonomy can have on the determinants of *trust*, *inclusion, citizen protection*, and *sustainability*.

These choices, while highly relevant, are meant to be illustrative, and similar analyses could be performed with other considerations.

1 Trust

Seen as a precondition for e-government system adoption (Carter & Weerakkody, 2008; Li et al., 2008; Warkentin et al., 2002; Welch et al., 2004), trust refers to 'the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the user, irrespective of the ability to monitor or control that other party'. It comprises three dimensions: benevolence, competence and integrity (Mayer et al., 1995, p. 95). This is of particular importance in the context of digital identification (Okunoye, 2022), as many high-level institutions have realized, appending the word 'trusted' to 'digital identity' in their communications (Australian Government, 2023; European Commission, 2021b; World Bank, 2019b). Li et al. (2008) empirically studied the determinants and impacts of trust in intended usage of national identification systems to get a more nuanced understanding of which aspects of trust lead to intended usage of national digital identity systems. Three key factors influencing trust beliefs were identified. The first is system reputation, which refers to the system's perceived benevolence, competence, and reliability. The second is system calculated cost-benefit, which considers whether the system or the responsible organization stands to gain from engaging in malevolent, incompetent, or dishonest behavior. The third is organizational institution situation normality, which pertains to the responsible organization's perceived benevolence, competence, and integrity. Linking these determinants to the choices that governments are facing when developing digital identity infrastructure correlates with the insights gathered during our data collection. Trust levels have been associated with governance decisions in comparative studies of HICs digital identity implementations (Kubicek & Noack, 2010b). Applying this lens to our taxonomy, it could be derived that trusting beliefs could indeed be impacted by the choices made within the *authority governance model*, *additional authority prerogatives*, *roles of private actors*, *development funding*, *data presentation model, identity matching approach* and *trusted sources* dimensions.

Both the choices within the *authority governance model* and *additional authority prerogatives* dimensions impact the organizational situation normality determinant. The authority will inevitably be associated with the institution in charge, and its societal role. As such, affiliating the authority to a trusted ministry or directly to a popular head of state will have a positive impact on the trust beliefs attributed to the infrastructure (Kubicek & Noack, 2010a). On the contrary, associating the infrastructure with unpopular ministries or prerogatives would negatively influence them. In LMICs, informal institutions such as religious and traditional leaders can be more trusted than formal institutional actors (Bratton & Gyimah-Boadi, 2016). Involving them in the governance of the authority, e.g., through board positions, could then influence citizens' trust. In Guinea for example, the board of the authority responsible for digital identity (ONECI) comprises a representative of religious affairs (Présidence de la République de Guinée, 2022), strengthening public trust in the system in a context where religion plays a central role in daily life and governance.

The choices made in the dimension *roles of private actors* can also be particularly impactful, as exemplified by the overwhelming rejection of Swiss voters to a digital identity infrastructure primarily managed by the private sector (Swiss Federal Counsel, 2021). This led to a dramatic reversal of fate, with a new proposal severely limiting the roles of private sector actors now adopted by the Swiss Federal Counsel (Swiss Federal Counsel, 2023). However, one should not equate private sector with untrustworthiness. In Nigeria for example, poor government performance is a determining factor in the current lack of trust in the national identity system (Okunoye, 2022). Trust in the public and private sector is geography dependent and highly volatile; in fact, there is a current worldwide trend towards a higher trust in the private sector than the public sector (Edelman, 2023). Determinants of success in public-private partnerships for digital infrastructure include engagement, joint understanding, two-way communication, clear division of roles and following a process-oriented approach (Lips et al., 2023). Trust however does not exclude control, and as the experience of India shows, clear control and monitoring of arrangements with the private sector can help this trust last, in particular for citizen-facing activities such as enrolment (CAG of India, 2021).

Development funding is another trust-affecting dimension, in particular in LMICs where external funding is often necessary to develop the infrastructure. Loans can be associated with dependency and a loss of sovereignty, whether they come from international financial institutions (Williams, 2000) or private capital markets (Leiteritz, 2001). However, foreign aid has also been a positive vector of citizen trust in countries where trust in government is low (Milner et al., 2016). Public-private agreements, such as build-own-transfer and concession agreements, can also have a similar association and impact the *system calculated cost/benefit* trust determinant (Feng et al., 2018). They can also activate the kinds of dynamics highlighted within the *roles of private actors* dimension.

Data presentation model, identity matching approach and *trusted sources* can all impact the *system reputation* determinant by introducing technological trust mediators, i.e., digital technologies that mediate interactions that require or produce trust, despite the lack of evidence with respect to the actual trustworthiness of these mediators (Bodó, 2021). While these trust-mediating technologies are increasingly used in LMICs (e.g., Brazil's use of distributed ledger technology, Bhutan's use of digital credentials and wallets), understanding their implications require significant digital literacy. As such, while they might be influencing trust in highly digital literate societies, this effect cannot be presumed in all contexts.

2 Inclusion

Inclusion is a second challenge that was often referred to in the data we collected and analyzed (uncoincidentally, another word often appended to digital identity (UNHCR, 2018; USAID, 2017; World Bank, 2019b). Digital identity infrastructure was highlighted as a potential vector of both inclusion and exclusion, an observation that finds confirmation in the academic literature (Bannister & Connolly, 2014; Beduschi, 2019; Martin & Taylor, 2021; Masiero & Arvidsson, 2021). In a governmental program context, it relates to data justice, equity, fairness and service to the citizen (Bannister & Connolly, 2014). For simplicity purposes, both inclusion and lack of exclusion will be equally considered here, although there is nuance to their meaning and impacts (Cicchiello et al., 2021). Inclusion is impacted by choices made within the *authority governance model*, *additional authority prerogatives*, *subjects*, *geographical scope*, *interoperability approach*, *operational financing, data presentation model* and *trusted sources* dimensions.

Within the *authority governance model* and *additional authority prerogatives* dimensions, governments can manage the risk of exclusion through different institutional arrangements, such as granting governance prerogatives to stakeholders with social inclusion improvement in their mandate. These responsibilities can be at the programmatic, project or informal level. Once again, the board of Guinea's ONECI comprises a representative of the ministry in charge of the advancement of women, children and vulnerable persons. In Sierra Leone, the entity already responsible for the enrolment of the population (NCRA) was given the additional prerogative of establishing the digital identity infrastructure. But inclusion is not unidirectional, and institutional arrangements ignoring this risk can also reinforce existing systemic exclusion. For example, too strong a link between documentation, registration and the provision of social benefits can lead to cascading exclusionary effects, and not accounting for unregistered people can lead to trickle-down effects of the implementation of social policies (Chudnovsky & Peeters, 2021). This is exemplified by the example of the Nubian community, who due to the history of their arrival in Kenya, struggled to fulfil the requirements for enrolling in the digital identity infrastructure, subsequently depriving them of access to essential services (Mosero, 2021). In a similar dynamic, the registration of newborns in South Africa was conditioned to the possession of valid documentation, generating cascading generational exclusion (ibid.).

The *subjects*, *geographical scope* and *interoperability approach* dimensions deal with the aspects of demographic and geographic inclusion. Choices made with regards to the category of population eligible to interact with governmental or private services due to their (non-) integration in the digital identity infrastructure has considerable ethical, if not legal, implications of data justice (Bhatia et al., 2021; Schoemaker et al., 2021; Tavares & Masiero, 2023), that need to be taken into consideration before deciding on this dimension. It also raises practical questions regarding the enrolment of target data subjects and reinforces the need to carefully evaluate how integration with existing systems (e.g., civil registration, vital statistics, identity document issuance) is apprehended, to avoid 'cascades of exclusion' for persons who are not included in the digital identity program (Chudnovsky & Peeters, 2021). In LMICs where forced displacement-causing conflicts are likely to occur, cross-border interoperability can alleviate the risks of exclusion of displaced populations not having their legal identity recognized by host countries (Martin & Taylor, 2021; World Bank, 2023a). Risks to inclusion are compounded by digital identity infrastructures' increasing reliance on the biometric information of data subject, as this highly sensitive category of personal data can allow precise identification (Cooper & Yon, 2019; Mankoff et al., 2022; Wickins, 2007). Indeed, quality of certain biometrics can be impacted by different factors including age, health conditions or even position on the urban-rural continuum (Huang et al., 2019; Lanitis, 2010; Tiwari & Gupta, 2014), which increases the risk of certain populations to be excluded from biometrics-based digital identity schemes.

Within the *operational financing*, *data presentation model* and *trusted sources* lie inclusion challenges due to varying availability of citizen resources, such as digital literacy and income, that are particularly prevalent in LMIC (Antonio & Tuffley, 2014; Mathrani et al., 2022; Our World In Data, 2023; Zdjelar & Žajdela Hrustek, 2021). Charges for data subjects are usually seen as a potential exclusion vector because of the financial barriers they create (World Bank, 2019a), although they can achieve precisely the opposite when used appropriately (Thomas, 1998). Digital wallets, thanks to their remote delivery capabilities, can be useful in reducing the often-significant costs (including opportunity costs) of reaching and waiting at enrolment or credentials distribution centers. They can also be useful in situations where internet connectivity is limited, a pervasive issue in regions where people are at the highest risk of exclusion. However, they often presume ownership of a sophisticated, costly piece of hardware – typically a smartphone (Schoemaker et al., 2023). While techniques have been proposed to bridge the newer capabilities available through digital identification with legacy phone hardware (Mavroudis et al., 2021), the secure element and trusted execution environment necessary to enable highly-secure identity transactions can only be found in specialized hardware or recent smartphones (ENISA, 2020). Alternatives such as the Indian offline e-KYC model can alleviate some of the hardware ownership requirements, but their usage also presumes a sufficient level of digital literacy (International Center for Humanitarian Affairs, 2021), thus generating additional risks of exclusion if not handled appropriately.

3 Citizen protection

Digital identity infrastructures are built to process personal data with the purpose of accessing individualized services, and the risks of misuse are not to be underestimated. Aside from protection from exclusion (addressed within the inclusion challenge), citizen protection in the context of digital identification was mainly reported as being concerned with protection from data misuse such as surveillance. Masiero (2023) comments that surveillance is inevitable and composes the fabric of digital identity systems, and Thoburn (2012) considers that identification is de facto a benign form of surveillance which is required for a well-ordered society. Weitzberg et al. (2021) appeals to a depolarized approach, suggesting that surveillance and recognition are mutually compatible developments. This position is shared by Taylor et al. (2008) who calls for a contextual perspective and a holistic understanding of the relationship between public service provision and surveillance to propose practical routes and reconciliations between naïve optimism about the roles of government and the 'dark spectres' attaching to them. Beyond surveillance at the systemic level, data misuse can include discrimination and identity theft, and can occur at the organizational or individual level, by leveraging legitimately or illegitimately collected data (Lowry et al., 2017; Robertson, 2019). All types of data misuse can have a substantial impact on the targeted data subject (Kröger et al., 2021). Citizen protection is impacted by choices made within the *authority governance model*, *additional authority prerogatives*, *geographical scope*, *interoperability enablers*, *roles of private sector actors, data presentation model, identity matching approach* and *trusted sources* dimensions.

The *authority governance model*, *additional authority prerogatives*, *geographical scope* and *roles of private sector actors* dimensions are all concerned with who can have access to identification data, or at least who can decide on it. De-linking identification from other prerogatives that could have incentives to misuse identity data (Lai & Patrick Rau, 2021; Radiya-Dixit & Neff, 2023) could act as a rudimentary protection against this risk. The private sector often has systemic incentives to leverage this personal data for uses beyond their originally intended purposes (Kröger et al., 2021; Prichard, 2021). But the public sector is not always beyond reproach, and misuse has been reported at the individual level (Hutchings & Jorna, 2015; Inuwa et al., 2019), as well as at the organizational level (Bannister, 2005; Königs, 2022; Taylor et al., 2008). In the Netherlands, any identification transaction needs to go through an authorization system, which verifies the legal basis for data processing and limits data access strictly to the necessary. It also leverages techniques known as polymorphic encryption and pseudonymization to prevent data reconciliation through an identifier (Verheul & Jacobs, 2017). Despite its complexity, this combination of *authority governance model* and *identity matching approach* can be an example of a way of data misuse, the principles of which being also found in Austria (Kubicek & Noack, 2010b) and India (Ministry of Justice, India, 2019), for example, with identifier tokenization and virtual IDs.

Interoperability enablers configurations can also be leveraged to impact citizen protection capabilities. Both the use of standards and open-source / community software presents the advantage of being open to full scrutiny. Functioning on the premise of security via transparency, they have the potential to enhance system security (Hoepman & Jacobs, 2007; Witten et al., 2001). But while some evidence points to this dynamic, direct causation has yet to be proven, and proprietary developments might provide better security than obscure standards or little-scrutinized open-source projects (Hansen et al., 2002; Sridhar et al., 2005). Finally, *certification and accreditation mechanisms* leverage oversight by a qualified institution to reduce the risk that external partners or resources present risks to citizens. For example, in India, Aadhaar enrolment personnel need to go through a certification process before being authorized to act as a registrar on behalf of the government (UIDAI, 2022).

The *data presentation model, identity matching approach* and *trusted sources* dimensions are concerned with the relationship between data subjects and infrastructure actors. A framework that establishes the conditions in which data matching is allowed to take place can help avoid cases of illegitimate data matching and inferences (Wachter & Mittelstadt, 2018). This however presents little protection in case a unique identifier is openly used and shared, such as the National Identity Number in Nigeria (NIMC, 2022). A glimpse into HICs implementations may provide insight into future directions of this topic: during the eIDAS revision process, the proposed introduction of a unique and persistent identifier was rolled back following intense pushback from privacy advocates and data protection authorities (European Parliament, 2023). Consideration to introduce unique identifiers should then be well-informed, considering the tradeoff required between simplicity of usage and data protection risks. Biometrics, as identity data that can enable identity matching, can also be used to deduce health conditions (Ross et al., 2022) and ethnicity (AlBdairi et al., 2022) characteristics prone to be used to discriminate against individuals, in particular in LMICs (Gavan et al., 2022). Although their efficacy in achieving user empowerment is debated (Giannopoulou, 2023), digital wallets are currently being presented as preferable to a more siloed approach from a privacy preservation standpoint (European Commission, 2025). They can be enhanced with privacy-enhancing technologies and permit selective disclosure, i.e., a technological implementation of the data minimization principle (Veseli et al., 2019). Regarding distributed ledgers, while they can be seen as opportunities for trust mediation in collaborative contexts, caution is advised against storing anything but technical data for purposes such as proof verification, schemas management and rules enforcement (Ghaffari et al., 2022; Lux et al., 2020; Sim et al., 2019), due to their incapacity to guarantee several data protection rights, such as the rights to erasure or rectification.

4 Sustainability

In this context, *sustainability* is considered as the challenge of maintaining the desirable characteristics of the infrastructure over time, from both a financial and outcome-based perspective. While sustainability understood as environmentalism is a critical topic in information technology (Sarkis et al., 2013; Seidel et al., 2017), the choices identified in this study were not considered as having a direct impact on the ecological footprint of the infrastructure (including when considering decentralized ledger technologies as long as an appropriate consensus mechanism is used (Sedlmeir et al., 2020)). In practice, sustainability (also called *long-term future*) is one of the key considerations for the project appraisal of funding towards digital identity (UNCDF, 2020; World Bank, 2019c). The UK offers a cautionary tale in the dangers of program unsustainability, with their flagship GOV.UK Verify program being fully discontinued in 2023 due to low usage and unclear prerogatives, despite substantial investment and commitment to the infrastructure (National Audit Office, 2019). While the UK had fallback measures in place, this example highlights the real risks citizens in LMICs face should governmental service provision depend on an unsustainable foundational identity infrastructure.

The dimensions affecting program sustainability are primarily *authority governance model, interoperability enablers, development funding, operational financing, data presentation model, identity matching approach* and *trusted sources.*

The choice of the *authority governance model* can have an impact on the political resilience of the infrastructure. Regime instability is a reality that many LMICs have to face. As an example, three out of six countries taking part in the World Bank's West African Unique Identification for Regional Integration (WURI) program (a program which development objective is to increase the number of persons in participating countries who have government-recognized proof of unique identity that facilitates access to services) have been subject to one or several coups since the approval of the program in 2018 (Burkina Faso, Guinea and Niger). But sudden political change is not limited to sub-Saharan Africa (Manurung, 2021). Regime instability hampers infrastructural resilience due to the risk of sweeping changes in ministerial appointments and reduced infrastructural investments (Magwedere & Marozva, 2023). Reducing the dependence of the digital identity authority on other parts of government could alleviate some of these risks: for example, it has been proposed that making it a neutral service provider at the service of citizens will reduce its likelihood to be a lustration target (Shirlow, 2021). However, while this hypothesis has merit, it is yet to be empirically validated.

Interoperability enablers can primarily influence the financial sustainability of the program. The use of standards and open-source / community software can both reduce the investment in developing and maintaining the infrastructure (Fitzgerald & Kenny, 2004). This could in turn increase the resilience of the infrastructure during regime transition periods. However, the risk still exists that the maintenance budget for the infrastructure be cut regardless of the nominal costs. Use of open-source software and standards also make transitioning to new technological providers easier by alleviating vendor lock-in dynamics (Secure Identity Alliance, 2019; The Alan Turing Institute, 2021). This can improve resilience in cases when providers cease their activities, or do not deliver the expected benefits from the contractual arrangement. This in part directed the choice of countries to use open-source software for their digital identity infrastructure needs (e.g., Morocco and the Philippines' using MOSIP modules, and Madagascar, Ethiopia, Vietnam and Brazil using X-Road).

Choices made within the *development funding* and *operational financing* dimensions can directly impact financial sustainability through generic financial dynamics. Indeed, even with high expected rates of return (World Bank, 2018), reducing the initial necessary investment at the national level might create a future burden on public finances and hinder future investments (Ari & Koc, 2018; Woo & Kumar, 2015). Granting the digital identity authority the independence to generate their own revenues, including through inter-ministerial chargeback mechanisms, has been suggested as a means to reduce dependence on public budget (Gelb & Diofasi, 2018). However, so far, no empirical evidence has been collected to strongly support this hypothesis. Loan terms can also make a difference; between reports of 'debt trap diplomacy' effects (Carmody, 2020) and a sustainable development finance ideal lies an important grey area. A strategy employed by the World Bank to increase the likelihood of infrastructural success and resilience is to look beyond the infrastructure and consider prerequisites and outcomes. For example, fund disbursements can be conditioned to the establishment of a supporting legal framework and the issuance of identity credentials, on top of the building of the infrastructure (World Bank, 2018). When these terms are synergistic with the expected contextual outcome for the infrastructure provision, a higher chance of success could reasonably be expected.

Finally, *data presentation model*, *identity matching approach* and *trusted sources* can reduce dependence on governmental actors for the actualization of expected infrastructural benefits and thus impact their sustainability. Digital wallets are a typical example of disintermediation techniques that are often associated with independence from government, in particular since the coining of the term ‘self-sovereign identity’ (Giannopoulou, 2023). While it is true that in certain configurations, a digital credentials’ authenticity and integrity can be assessed without intervention of the issuer (W3C, 2022), in reality, a credential is only as good as an identity verifier’s trust in its validity, which only a trusted identity provider (i.e., the government in cases of legal identity) can attest. The use of a mediation service for identity matching can also add a sustainability risk, as it is in the critical path of an identification and authentication transaction, and it generates additional costs compared to the usage of a simple unique identifier.

5 Summary of impacts of governance design choices on benefits actualization

Based on this analysis, an illustrative mapping can be proposed that depicts how the taxonomy dimensions of (RP2) can impact the upholding of public values (RP5) in an LMIC context. Borrowing to Bannister et al. (2014), a table of hypotheses revealed by this instantiation of the taxonomy can be proposed. Despite its simplicity, this mapping allows for reaching two objectives: highlighting the interrelation between the taxonomy and pre-requisites for the actualization of benefits of digital identity infrastructure, as well as inviting both researchers and practitioners to explore the horizontal tensions that might evolve from them. As part of this discussion, are highlighted some choices that might have a positive impact on one pre-requisite, but a negative impact on another. For example, the fact that digital wallets could have a positive impact on citizen protection but a negative one on inclusion. Owing to the non-binary nature of these tensions (for example that charging citizens for the infrastructure could both have a negative and a positive impact on inclusion), future research accounting for the complexity of these dynamics would be warranted, to continue pursuing the goal of providing actionable guidance to conscientious designers and policymakers.

	Layer	Dimension	Impact identification			
			Trust	Inclusion	Citizen protection	Sustainability
Strategic Institutional and Governance Choices for Digital Identity Infrastructure	Institutional Arrangement	Authority governance model	✓	✓	✓	✓
		Additional authority prerogatives	✓	✓	✓	
	Ecosystem Management	Subjects		✓		
		Geographical scope		✓	✓	
		Interoperability approach		✓		
		Interoperability enablers			✓	✓
		Roles of private sector actors	✓		✓	
	Funding Management	Development funding	✓			✓
		Operational financing		✓		✓
	Data Management	Data presentation model	✓	✓	✓	✓
		Identity matching approach	✓		✓	✓
		Trusted sources	✓	✓	✓	✓

Table 4: Expected impacts of design choices on the pre-requisites for actualization of digital identity infrastructure benefits.

IV | Conclusion

This cumulative thesis examined digital public infrastructure from a human-centered perspective. It addressed the question of how policy makers and service designers can apprehend governance and institutional decisions when deploying digital identity infrastructure with a human-centered approach.

It did so by establishing an updated scientific understanding of public values and human-centeredness in the context of digital public services, by refining and broadening them (RP4; RP5). It then expanded comprehension of the dynamics behind successful adoption of digital identity infrastructure policy, by analyzing the case of the EU Digital Identity Framework (RP3).

With this theoretical basis covered, it then developed a framework for concisely apprehending strategic governance and institutional choices when designing digital identity infrastructure, through the elaboration of a consensus-based taxonomy (RP1; RP2), answering to the first research question of this thesis.

Finally, it applied this framework to assess the impact of design decisions on upholding public values. It did so through a case study of Aadhaar, India's digital identity infrastructure (RP2), and by evaluating four public values deemed particularly significant in the context of digital identity infrastructure.

All in all, I have (co-)authored 6 research papers and 1 book chapter that have contributed to answer the research questions of this thesis. The following subsections detail my research contributions, followed by a discussion of potential limitations and future research directions. The dissertation concludes by acknowledging prior work and situating it within the broader efforts of the FINATRAX research group at the Interdisciplinary Center for Security, Reliability, and Trust (SnT) at the University of Luxembourg.

1 Contributions

In an ever-complexifying context where technology is not simply considered for its affordances, but for the societal impact it generates, policymakers and service designers need tools to concisely apprehend how the governance choices they make can impact the outcome of their digital infrastructure. This thesis fills several important gaps in that respect.

First, it offers a structured and updated perspective on public values relevant to the digital age (RP4, RP5). Moving beyond enumeration, it establishes an analytical framework to investigate conflicts between user-centric approaches and public values in the domain of eGovernment. By identifying and categorizing conflict sources and dimensions, it provides a nuanced understanding of prevalent challenges in eGovernment initiatives. This analytical depth aims to inform both researchers and practitioners, highlighting critical areas requiring attention to ensure that user-centric approaches remain aligned with public values. Ultimately, this framework sensitizes stakeholders to the inherent tensions, fostering more effective and value-oriented eGovernment solutions.

Second, it delivers actionable insights into policy-making strategies for large-scale digital identity programs (RP3). It demonstrates the applicability of punctuated equilibrium theory (Baumgartner et al., 2018; Baumgartner & Jones, 2009) while extending and refining its implications in the European context. This analysis is particularly beneficial for countries aiming to secure successful adoption of strategies and policies for digital identity systems. These insights guide policymakers in navigating complex socio-political landscapes, ensuring context-aware and federating implementation. Moreover, this contribution adds granularity to the understanding of policy evolution in the digital identity domain, offering an analytical lens that bridges academic inquiry and practical application.

Third, by introducing and instantiating a taxonomy (RP1, RP2), this work provides a robust framework for analyzing digital identity governance decisions. This taxonomy can serve as a tool for researchers to generalize, communicate, and apply findings systematically, enhancing theory-building in areas such as eGovernment digital infrastructure and broader information systems research. Practitioners can also leverage this framework to navigate governance challenges more effectively, distinguishing strategic elements of digital identity infrastructures in a systematic manner. Additionally, this taxonomy equips policymakers with a concise analytical tool to evaluate design choices, offering practical guidance during the design and implementation phases. For citizens, the taxonomy enhances transparency, empowering them to better understand governance decisions and engage in participatory actions that influence infrastructure development.

Finally, the instantiation of the taxonomy in section III of this thesis sheds light on critical governance considerations, such as public-private sector arrangements, while raising questions for future research—particularly regarding how governance decisions impact benefit realization in digital identity infrastructures. This opens avenues for comparative empirical studies that generate actionable insights for both researchers and practitioners.

2 Limitations and Outlook

Naturally, the individual research items composing this thesis have certain limitations, which open opportunities for further research to refine and expand the findings of this thesis.

The findings of RP1 and RP2 are influenced by contextual factors, particularly in the taxonomy's reliance on analyzed cases and expert interviews, which may affect its generalizability across diverse contexts. Additionally, the empirical validation in real-world deployments presents opportunities for further exploration. Future extensions that incorporate emerging technological and governance developments will not only enrich their utility but also ensure their continued relevance in dynamic contexts. Taxonomies also have inherent limitations, as they do not have truth value, but are rather tools for utility. While it resonated with interview participants, its complexity could pose challenges for those unfamiliar with the field. Additionally, a more systematic evaluation of digital identity infrastructures could uncover rare characteristics worth including. To address these limitations, further research could provide case-study evaluations of governance decisions' impacts and explore the interplay between governance and technical elements. Deeper investigation into the taxonomy's dimensions and adopting a reverse innovation approach could also offer valuable insights from developing countries applicable to high-income contexts. The taxonomies having been designed with extensibility in mind, should allow them to adapt and evolve alongside changes in implementation paradigms.

RP3 uses process tracing, a method recognized for its rigor and effectiveness when applied in complex research domains (Ricks & Liu, 2018). However, the reliance on elite interviews and documentation that is necessarily steered by personal and institutional agendas, may provide a skewed perspective on the policy-making processes at hand. Additionally, its Eurocentric scope could limit its application to other global or regional initiatives. Expanding the analysis to include non-EU contexts would provide a more comprehensive understanding of policy development. Further exploration of the interplay between policy punctuations and technological evolution, as well as incorporating citizen and private-sector stakeholder roles, could contribute to deepen the insights offered.

RP4 and RP5 both draw on existing scientific literature as a research foundation, incorporating insights from over 70 research projects to provide consolidated theoretical findings. While this reliance benefits its breadth, it limited how far these research papers could engage with emerging technologies like AI and blockchain, which are increasingly relevant in this context and have the potential to alter conceptions of human-centered approaches. Additionally, these findings would benefit from empirical validation through case studies. Future research could address these gaps by conducting detailed case studies on recent eGovernment projects that explore the practical implications of the dynamics identified in these studies.

Finally, RP6 takes a practical approach by designing a mobile application for refugee document management. By applying the design science research method, it ensures the relevance of findings to the case at hand (Hevner et al., 2004; Peffers et al., 2007). However, the study's reliance on a limited sample of interviews and its focus on European settings limit its generalizability to other contexts. These aspects could be further extended to capture more diverse contexts. Future research could explore broader geographical and cultural settings and undertake longitudinal studies to evaluate the long-term impact of such applications on refugee trust and integration. Additionally, with the field of privacy-preserving technologies evolving at a rapid pace, updates of the proposed design taking them into account could further strengthen trust and encourage adoption among refugees.

3 Acknowledgement of Previous and Related Work

The research papers presented in this thesis are the outcome of collaborations with researchers from the University of Luxembourg, the University of Bayreuth, the University of Augsburg, the University of Zurich and the University of Milan.

In particular, the Finatrax research collective produced substantial work on digital identity privacy, governance and semantic considerations (Babel & Sedlmeir, 2023; Barbereau & Bodó, 2023; Feulner et al., 2022; Garrido et al., 2022; Glöckler et al., 2023; Guggenberger et al., 2023; Rieger et al., 2022; Roth et al., 2024; Sartor et al., 2022; Schlatt et al., 2021; Sedlmeir et al., 2021, 2022, 2023, 2023; Smethurst, 2023; Weigl, Barbereau, Rieger, et al., 2022a; Weigl et al., 2023). The research on public values and on refugees took place in exchange with the research of (Casalini & Zavolokina, 2023; Garazha et al., 2024; Zavolokina et al., 2023), and the work stream on public policy benefitted from the research of (Codagnone & Weigl, 2023).

V | References

50-in-5. (2023). Implementing digital public infrastructure, safely and inclusively. 50-in-5. https://50in5.net/

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for Development : Digital Identification and its Link to Socioeconomic Inclusion. Government Information Quarterly.

AlBdairi, A. J. A., Xiao, Z., Alkhayyat, A., Humaidi, A. J., Fadhel, M. A., Taher, B. H., Alzubaidi, L., Santamaría, J., & Al-Shamma, O. (2022). Face Recognition Based on Deep Learning and FPGA for Ethnicity Identification. Applied Sciences, 12(5), Article 5. https://doi.org/10.3390/app12052605

Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. Data & Policy, 3, e35. https://doi.org/10.1017/dap.2021.35

Antonio, A., & Tuffley, D. (2014). The Gender Digital Divide in Developing Countries. Future Internet, 6(4), 673-687. https://doi.org/10.3390/fi6040673

Ari, I., & Koc, M. (2018). Sustainable Financing for Sustainable Development : Understanding the Interrelations between Public Investment and Sovereign Debt. Sustainability, 10(11), Article 11. https://doi.org/10.3390/su10113901

Australian Government. (2023). Trusted Digital Identity Framework (TDIF) | Digital Identity. https://www.digitalidentity.gov.au/tdif

Babel, M., & Sedlmeir, J. (2023). Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs (No. arXiv:2301.00823). arXiv. http://arxiv.org/abs/2301.00823

Bannister, F. (2005). The panoptic state : Privacy, surveillance and the balance of risk. Information Polity, 10(1,2), 65-78. https://doi.org/10.3233/IP-2005-0068

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government : A framework and programme for research. Government Information Quarterly, 31(1), 119-128. https://doi.org/10.1016/j.giq.2013.06.002

Barbereau, T., & Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software : In search of secondary liability. Computer Law & Security Review, 49. https://doi.org/10.1016/j.clsr.2023.105829

Bason, C. (2017). Leading public design : Discovering human-centred governance (1re éd.). Bristol University Press. https://doi.org/10.2307/j.ctt1t88xq5

Baumgartner, F. R., & Jones, B. D. (2009). Agendas and Instability in American Politics, Second Edition. University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/A/bo6763995.html

Baumgartner, F. R., Jones, B. D., & Mortensen, P. B. (2018). Punctuated Equilibrium Theory : Explaining Stability and Change in Public Policymaking. In Theories of the Policy Process (4e éd.). Routledge.

Beduschi, A. (2019). Digital identity : Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 205395171985509. https://doi.org/10.1177/2053951719855091

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies : Data privacy and human rights considerations. Data & Policy, 3. https://doi.org/10.1017/dap.2021.15

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. The Journal of Strategic Information Systems, 17(2), 165-176. https://doi.org/10.1016/j.jsis.2007.12.002

Bhatia, A., Donger, E., & Bhabha, J. (2021). 'Without an Aadhaar card nothing could be done' : A mixed methods study of biometric identification and birth registration for children in Varanasi, India. Information Technology for Development, 27(1), 129-149. https://doi.org/10.1080/02681102.2020.1840325

Bocchini, P., Frangopol, D. M., Ummenhofer, T., & Zinke, T. (2014). Resilience and Sustainability of Civil Infrastructure : Toward a Unified Approach. Journal of Infrastructure Systems, 20(2), 04014004. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000177

Bodó, B. (2021). Mediated trust : A theoretical framework to address the trustworthiness of technological trust mediators. New Media & Society, 23(9), 2668-2690. https://doi.org/10.1177/1461444820939922

Bratton, M., & Gyimah-Boadi, E. (2016). Do trustworthy institutions matter for development ? Corruption, trust, and government performance in Africa. https://www.afrobarometer.org/wp-content/uploads/migrated/files/publications/Dispatches/ab_r6_dispatchno112_trustworthy_institutions_and_development_in_africa.pdf

Bruijn, H. D., & Dicke, W. (2006). Strategies for Safeguarding Public Values in Liberalized Utility Sectors. Public Administration, 84(3), 717-735. https://doi.org/10.1111/j.1467-9299.2006.00609.x

Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2014). Public Value Governance : Moving Beyond Traditional Public Administration and the New Public Management. Public Administration Review, 74(4), 445-456. https://doi.org/10.1111/puar.12238

CAG of India. (2021). Report of the Comptroller and Auditor General of India on the Functioning of Unique Identification Authority of India. https://cag.gov.in/webroot/uploads/download_audit_report/2021/24%20of%202021_UIDAI-0624d8136a02d72.65885742.pdf

Carayon, P., Wooldridge, A., Hoonakker, P., Hundt, A. S., & Kelly, M. M. (2020). SEIPS 3.0 : Human-centered design of the patient journey for patient safety. Applied Ergonomics, 84, 103033. https://doi.org/10.1016/j.apergo.2019.103033

Carmody, P. (2020). Dependence not debt-trap diplomacy. Area Development and Policy, 5(1), 23-31. https://doi.org/10.1080/23792949.2019.1702471

Carter, L., & Weerakkody, V. (2008). E-government adoption : A cultural comparison. Information Systems Frontiers, 10(4), 473-482. https://doi.org/10.1007/s10796-008-9103-6

Casalini, F., & Zavolokina, L. (2023). Do collaborative platforms create public value in public services? An explorative analysis of privately-owned public service platforms in Italy. Casalini, Francesca; Zavolokina, Liudmila (2023). Do Collaborative Platforms Create Public Value in Public Services? An Explorative Analysis of Privately-Owned Public Service Platforms in Italy. In: 39th EGOS Colloquium, Cagliari, 4 July 2023 - 8 July 2023, 1-45., 1-45. https://doi.org/10.5167/uzh-234232

Chaudhuri, B. (2021). Distant, opaque and seamful : Seeing the state through the workings of Aadhaar in India. Information Technology for Development, 27(1), 37-49. https://doi.org/10.1080/02681102.2020.1789037

Chudnovsky, M., & Peeters, R. (2021). A cascade of exclusion : Administrative burdens and access to citizenship in the case of Argentina’s National Identity Document. International Review of Administrative Sciences, 88, 002085232098454. https://doi.org/10.1177/0020852320984541

Cicchiello, A. F., Kazemikhasragh, A., Monferrá, S., & Girón, A. (2021). Financial inclusion and development in the least developed countries in Asia and Africa. Journal of Innovation and Entrepreneurship, 10(1), 49. https://doi.org/10.1186/s13731-021-00190-4

Codagnone, C., & Weigl, L. (2023). Leading the Charge on Digital Regulation : The More, the Better, or Policy Bubble? Digital Society, 2. https://doi.org/10.1007/s44206-023-00033-7

Cooper, I., & Yon, J. (2019). Ethical Issues in Biometrics. Science Insights, 30(2), 63-69. https://doi.org/10.15354/si.19.re095

Dawes, S. S. (2009). Governance in the digital age : A research and action framework for an uncertain future. Government Information Quarterly, 26(2), 257-264. https://doi.org/10.1016/j.giq.2008.12.003

De Graaf, G., Huberts, L., & Smulders, R. (2016). Coping With Public Value Conflicts. Administration & Society, 48(9), 1101-1127. https://doi.org/10.1177/0095399714532273

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electronic Markets, 34. https://doi.org/10.1007/s12525-024-00731-1

de Graaf, G., & van der Wal, Z. (2010). Managing Conflicting Public Values : Governing With Integrity and Effectiveness. The American Review of Public Administration, 40(6), 623-630. https://doi.org/10.1177/0275074010375298

DPGA, & GiZ. (2022, mai). GovStack Definitions : Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf

Dunleavy, P. (2005). New Public Management Is Dead—Long Live Digital-Era Governance. Journal of Public Administration Research and Theory, 16(3), 467-494. https://doi.org/10.1093/jopart/mui057

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). Social Security : Managing Mass Payments and Responding to Welfare State change. In P. Dunleavy, H. Margetts, S. Bastow, & J. Tinkler (Éds.), Digital Era Governance : IT Corporations, the State, and e-Government (p. 0). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199296194.003.0007

Edelman. (2023). 2023 Edelman Trust Barometer. Edelman. https://www.edelman.com/trust/2023/trust-barometer

ENISA. (2020). eIDAS compliant eID solutions.

European Commission. (2021a). Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Official Journal of the European Union. https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission. (2021b, juin 3). Commission proposes a trusted and secure Digital Identity for all Europeans [Text]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

European Commission. (2025). Security and Privacy—EU Digital Identity Wallet. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security%2Band%2BPrivacy

European Parliament. (2023). 10 2023 | A Europe Fit for the Digital Age | Revision of the eIDAS Regulation – European Digital Identity (EUid).

Feng, K., Wang, S., Li, N., Wu, C., & Xiong, W. (2018). Balancing public and private interests through optimization of concession agreement design for user-pay PPP projects. Journal of Civil Engineering and Management, 24(2), Article 2. https://doi.org/10.3846/jcem.2018.455

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the Use of Self-sovereign Identity for Event Ticketing Systems. Electronic Markets, 32(3), Article 3. https://doi.org/10.1007/s12525-022-00573-9

Fitzgerald, B., & Kenny, T. (2004). Developing an information systems infrastructure with open source software. IEEE Software, 21(1), 50-55. https://doi.org/10.1109/MS.2004.1259216

Frederickson, H. G. (1990, mars 1). Public Administration and Social Equity. | EBSCOhost. https://doi.org/10.2307/976870

G20. (2023). Digital Economy Outcome Document and Chair's Summary. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20_Digital_Economy_Outcome_Document%20_and_Chair%27s_Summary_19082023.pdf

Garazha, A., Merz, C., Schwabe, G., & Zavolokina, L. (2024). Resilience in Times of Crisis : Empowering Refugees with Self-Sovereign Identity.

Garrido, G. M., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. (2022). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT : A systematic literature review. Journal of Network and Computer Applications, 207, 103465. https://doi.org/10.1016/j.jnca.2022.103465

Gasson, S. (2003). Human-Centered vs. User-Centered Approaches to Information System Design. Journal of Information Technology Theory and Application (JITTA), 5(2). https://aisel.aisnet.org/jitta/vol5/iss2/5

Gavan, L., Hartog, K., Koppenol-Gonzalez, G. V., Gronholm, P. C., Feddes, A. R., Kohrt, B. A., Jordans, M. J. D., & Peters, R. M. H. (2022). Assessing stigma in low- and middle-income countries : A systematic review of scales used with children and adolescents. Social Science & Medicine, 307, 115121. https://doi.org/10.1016/j.socscimed.2022.115121

Gelb, A., & Diofasi, A. (2018). Identification Revolution : Can Digital ID be Harnessed for Development?

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology : A survey. International Journal of Network Management, 32(2), e2180. https://doi.org/10.1002/nem.2180

Giannopoulou, A. (2020). Data Protection Compliance Challenges for Self-sovereign Identity. In J. Prieto, A. Pinto, A. K. Das, & S. Ferretti (Éds.), Blockchain and Applications (p. 91-100). Springer International Publishing.

Giannopoulou, A. (2023). Digital Identity Infrastructures : A Critical Approach of Self-Sovereign Identity. Digital Society, 2(2), 18. https://doi.org/10.1007/s44206-023-00049-z

Gil-Garcia, J. R. (2012). Enacting Electronic Government Success : An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions (Vol. 31). Springer US. https://doi.org/10.1007/978-1-4614-2015-6

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020). Towards a comprehensive understanding of digital government success : Integrating implementation and adoption factors. Government Information Quarterly, 37(4), 101518. https://doi.org/10.1016/j.giq.2020.101518

Glöckler, G., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering. https://doi.org/10.1007/s12599-023-00830-x

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a Cross-organizational Identity Management System : Utilizing SSI for the Certification of Retailer Attributes. Electronic Markets, 33(1), Article 1. https://doi.org/10.1007/s12525-023-00620-z

Gurara, D., Klyuev, V., Mwase, N., & Presbitero, A. F. (2018). Trends and Challenges in Infrastructure Investment in Developing Countries. International Development Policy | Revue Internationale de Politique de Développement, 10.1, Article 10.1. https://doi.org/10.4000/poldev.2802

Hansen, M., Köhntopp, K., & Pfitzmann, A. (2002). The Open Source approach—Opportunities and limitations with respect to security and privacy**This paper was presented at ISSE 2001, September 26–28, London. This version is slightly revised. Computers & Security, 21(5), 461-471. https://doi.org/10.1016/S0167-4048(02)00516-3

Heeks, R. (2002). Information Systems and Developing Countries : Failure, Success, and Local Improvisations. The Information Society, 18(2), 101-112. https://doi.org/10.1080/01972240290075039

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. MIS Quarterly, 37(3), 907-931.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 75-105.

Hoepman, J.-H., & Jacobs, B. (2007). Increased security through open source. Communications of the ACM, 50(1), 79-83. https://doi.org/10.1145/1188913.1188921

Holeman, I., & Kane, D. (2020). Human-centered design for global health equity. Information Technology for Development, 26(3), 477-505. https://doi.org/10.1080/02681102.2019.1667289

Hooda, A., Gupta, P., Jeyaraj, A., Giannakis, M., & Dwivedi, Y. K. (2022). The effects of trust on behavioral intention and use behavior within e-government contexts. International Journal of Information Management, 67, 102553. https://doi.org/10.1016/j.ijinfomgt.2022.102553

Huang, P., Guo, L., Li, M., & Fang, Y. (2019). Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare. IEEE Internet of Things Journal, 6(5), 9200-9210. https://doi.org/10.1109/JIOT.2019.2929087

Hundal, H. S., & Chaudhuri, B. (2020). Digital Identity and Exclusion in Welfare : Notes from the Public Distribution System in Andhra Pradesh and Karnataka. Proceedings of the 2020 International Conference on Information and Communication Technologies and Development, 1-5. https://doi.org/10.1145/3392561.3397583

Husz, O. (2018). Bank Identity : Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. Enterprise & Society, 19(2), 391-429. https://doi.org/10.1017/eso.2017.43

Hutchings, A., & Jorna, P. (2015). Misuse of information and communications technology within the public sector.

Inoue, T. (2024). Digital financial inclusion, international remittances, and poverty reduction. Journal of Economic Structures, 13(1), 8. https://doi.org/10.1186/s40008-024-00328-z

International Center for Humanitarian Affairs. (2021). DIGID Lessons Learnt from Kenya. https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

Inuwa, I., Ononiwu, C., Kah, M. M. O., & Quaye, A. K. M. (2019). Mechanisms Fostering the Misuse of Information Systems for Corrupt Practices in the Nigerian Public Sector. In P. Nielsen & H. C. Kimaro (Éds.), Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D (Vol. 552, p. 122-134). Springer International Publishing. https://doi.org/10.1007/978-3-030-19115-3_11

ISO 9241-210:2019. (2019). ISO. https://www.iso.org/standard/77520.html

ITU. (2018). Digital Identity Roadmap Guide. ITU. https://www.itu.int:443/en/publications/ITU-D/Pages/publications.aspx

Jones, N. N. (2016). Narrative Inquiry in Human-Centered Design : Examining Silence and Voice to Promote Social Justice in Design Scenarios. Journal of Technical Writing and Communication, 46(4), 471-492. https://doi.org/10.1177/0047281616653489

Jørgensen, T. B., & Bozeman, B. (2007). Public Values : An Inventory. Administration & Society, 39(3), 354-381. https://doi.org/10.1177/0095399707300703

Junginger, S. (2017). Transforming public services by design : Re-orienting policies, organizations and services around people. Routledge. https://doi.org/10.4324/9781315550183

Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. Philosophy & Technology, 35(1), 8. https://doi.org/10.1007/s13347-022-00503-9

Koppenjan, J., Charles, M. B., & Ryan, N. (2008). Editorial : Managing Competing Public Values in Public Infrastructure Projects. Public Money & Management, 28(3), 131-134. https://doi.org/10.1111/j.1467-9302.2008.00632.x

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. International Journal of Technology, Policy and Management, 5. https://doi.org/10.1504/IJTPM.2005.008406

Krippendorff, K. (2005). The Semantic Turn : A New Foundation for Design. CRC Press. https://doi.org/10.4324/9780203299951

Kröger, J. L., Miceli, M., & Müller, F. (2021). How Data Can Be Used Against People : A Classification of Personal Data Misuses. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3887097

Kubicek, H., & Noack, T. (2010a). Different countries-different paths. Extended comparison of the introduction of eIDs in eight European countries. Identity in the Information Society, 3. https://doi.org/10.1007/s12394-010-0063-x

Kubicek, H., & Noack, T. (2010b). The path dependency of national electronic identities. Identity in the Information Society, 3. https://doi.org/10.1007/s12394-010-0050-2

Kumar, R. L. (2004). A Framework for Assessing the Business Value of Information Technology Infrastructures. Journal of Management Information Systems, 21(2), 11-32. https://doi.org/10.1080/07421222.2004.11045801

Lai, X., & Patrick Rau, P.-L. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. Computers in Human Behavior, 124, 106894. https://doi.org/10.1016/j.chb.2021.106894

Lanitis, A. (2010). A survey of the effects of aging on biometric identity verification | International Journal of Biometrics. https://dl.acm.org/doi/10.1504/IJBM.2010.030415

Leiteritz, R. J. (2001). Sovereignty, developing countries and international financial institutions : A Reply to David Williams. Review of International Studies, 27(03). https://doi.org/10.1017/S0260210501004351

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. The Journal of Strategic Information Systems, 17(1), 39-71. https://doi.org/10.1016/j.jsis.2008.01.001

Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T., & Draheim, D. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership : Learning from the Case of Estonia. Information Systems Frontiers, 25(6), 2439-2456. https://doi.org/10.1007/s10796-022-10363-5

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact : Proposing a bold research agenda. European Journal of Information Systems, 26(6), 546-563. https://doi.org/10.1057/s41303-017-0066-x

Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020). Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 71-78. https://doi.org/10.1109/BRAINS49436.2020.9223292

Magwedere, M. R., & Marozva, G. (2023). Does political risk matter for infrastructure investments? Empirical evidence. Development Studies Research, 10(1), 2146596. https://doi.org/10.1080/21665095.2022.2146596

Mankoff, J., Kasnitz, D., Studies, D., Camp, L. J., Lazar, J., & Hochheiser, H. (2022). Areas of Strategic Visibility : Disability Bias in Biometrics. https://doi.org/10.48550/ARXIV.2208.04712

Manny, L., Angst, M., Rieckermann, J., & Fischer, M. (2022). Socio-technical networks of infrastructure management : Network concepts and motifs for studying digitalization, decentralization, and integrated management. Journal of Environmental Management, 318, 115596. https://doi.org/10.1016/j.jenvman.2022.115596

Manoharan, A. P., Melitski, J., & Holzer, M. (2023). Digital Governance : An Assessment of Performance and Best Practices. Public Organization Review, 23(1), 265‑283. https://doi.org/10.1007/s11115-021-00584-8

Manurung, H. (2021). Myanmar Political Instability : A Threat to Southeast Asia Stability. Jurnal Asia Pacific Studies, 5. https://doi.org/10.33541/japs.v5i1.2671

Martin, A., & Taylor, L. (2021). Exclusion and inclusion in identification : Regulation, displacement and data justice. Information Technology for Development, 27(1), 50‑66. https://doi.org/10.1080/02681102.2020.1811943

Masiero, S. (2018). Explaining trust in large biometric infrastructures : A critical realist case study of India's Aadhaar project. THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES, 84(6), e12053. https://doi.org/10.1002/isd2.12053

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. Information Systems Journal, 31(6), 903‑928. https://doi.org/10.1111/isj.12351

Mathrani, A., Sarvesh, T., & Umer, R. (2022). Digital divide framework : Online learning in developing countries during the COVID-19 lockdown. Globalisation, Societies and Education, 20(5), 625‑640. https://doi.org/10.1080/14767724.2021.1981253

Mavroudis, V., Hicks, C., & Crowcroft, J. (2021). An Interface Between Legacy and Modern Mobile Devices for Digital Identity. In A. Saracino & P. Mori (Éds.), Emerging Technologies for Authorization and Authentication (p. 68‑76). Springer International Publishing. https://doi.org/10.1007/978-3-030-93747-8_5

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 709. https://doi.org/10.2307/258792

McKinsey. (2019). Digital identification : A key to inclusive growth.

Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of power inscription into governance : Lessons from two national digital identity systems. Information Systems Journal, 32(2), 242-277. https://doi.org/10.1111/isj.12325

Milner, H. V., Nielson, D. L., & Findley, M. G. (2016). Citizen preferences and public goods : Comparing preferences for foreign aid and government programs in Uganda. The Review of International Organizations, 11(2), 219-245. https://doi.org/10.1007/s11558-016-9243-2

Ministry of Justice, India. (2019). The Aadhaar and other laws (amendment) Act 2019. https://uidai.gov.in/images/news/Amendment_Act_2019.pdf

Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing Digital Identity Goals – The Case Study of Aadhaar in India. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, & M. Mäntymäki (Éds.), Digital Transformation for a Sustainable Society in the 21st Century (Vol. 11701, p. 489-501). Springer International Publishing. https://doi.org/10.1007/978-3-030-29374-1_40

Mosero, R. (2021). Analysing the impact of Digital ID frameworks on Marginalised Groups in Sub-Saharan Africa. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3797506

Mothobi, O., & Grzybowski, L. (2017). Infrastructure deficiencies and adoption of mobile money in Sub-Saharan Africa. Information Economics and Policy, 40, 71-79. https://doi.org/10.1016/j.infoecopol.2017.05.003

Nabatchi, T. (2012). Putting the "Public" Back in Public Values Research : Designing Participation to Identify and Respond to Values. Public Administration Review, 72(5), 699-708. https://doi.org/10.1111/j.1540-6210.2012.02544.x

National Audit Office. (2019). Investigation into Verify (Summary).

Niemelä, M., & Melkas, H. (2019). Robots as Social and Physical Assistants in Elderly Care. In M. Toivonen & E. Saari (Éds.), Human-Centered Digitalization and Services (p. 177-197). Springer Nature. https://doi.org/10.1007/978-981-13-7725-9_10

Nihei, M. (2022). Epistemic Injustice as a Philosophical Conception for Considering Fairness and Diversity in Human-centered AI Principles. Interdisciplinary Information Sciences, 28(1), 35-43. https://doi.org/10.4036/iis.2022.A.01

NIMC. (2022). Data Privacy via Tokenization. Nigeria Data Privacy Initiative. https://wiki.nimc.gov.ng/en/privacy/data-protection/tokenization

Norman, D. A. (1988). The psychology of everyday things (p. xi, 257). Basic Books.

OECD. (2023). Recommendation of the Council on the Governance of Digital Identity. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

Okunoye, B. (2022). Mistrust of government within authoritarian states hindering user acceptance and adoption of digital IDs in Africa : The Nigerian context. Data & Policy, 4. https://doi.org/10.1017/dap.2022.29

Our World In Data. (2023). Income inequality vs. GDP per capita. Our World in Data. https://ourworldindata.org/grapher/gini-coefficient-vs-gdp-per-capita-pip?xScale=linear&time=2020

Park, S., & Humphry, J. (2019). Exclusion by design : Intersections of social, digital and data exclusion. Information, Communication & Society, 22(7), 934-953. https://doi.org/10.1080/1369118X.2019.1606266

Parliament of Bhutan. (2023). National_Digital_Identity_Act_of_Bhutan_2023F.pdf. https://www.nab.gov.bt/assets/uploads/docs/acts/2023/National_Digital_Identity_Act_of_Bhutan_2023F.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. New Media & Society, 20(1), 293-310. https://doi.org/10.1177/1461444816661553

Présidence de la République de Guinée. (2022). Decret D-2022-0134 portant création, attributions et fonctionnement de l'ONECI.

Prichard, E. C. (2021). Is the Use of Personality Based Psychometrics by Cambridge Analytical Psychological Science's "Nuclear Bomb" Moment? Frontiers in Psychology, 12, 581448. https://doi.org/10.3389/fpsyg.2021.581448

Radiya-Dixit, E., & Neff, G. (2023). A Sociotechnical Audit : Assessing Police Use of Facial Recognition. 2023 ACM Conference on Fairness, Accountability, and Transparency, 1334-1346. https://doi.org/10.1145/3593013.3594084

Rahaman, A., & Sasse, M. A. (2010). A framework for the lived experience of identity. Identity in the Information Society, 3(3), 605-638. https://doi.org/10.1007/s12394-010-0078-3

Ranchordas, S. (2020). Connected but Still Excluded? Digital Exclusion beyond Internet Access (SSRN Scholarly Paper No. 3675360). Social Science Research Network. https://doi.org/10.2139/ssrn.3675360

Ricks, J. I., & Liu, A. H. (2018). Process-Tracing Research Designs : A Practical Guide. PS: Political Science & Politics, 51(4), 842-846. https://doi.org/10.1017/S1049096518000975

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not Yet Another Digital Identity. Nature Human Behaviour, 6(1), Article 1. https://doi.org/10.1038/s41562-021-01243-0

Robertson, V. H. S. E. (2019). Excessive Data Collection : Privacy Considerations and Abuse of Dominance in the Era of Big Data (SSRN Scholarly Paper No. 3408971). https://doi.org/10.2139/ssrn.3408971

Røhnebæk, M. T., Engen, M., & Eide, T. H. (2019). Institutional Logics in Service Ecosystems : An Analysis of Immigration and Social Inclusion. In M. Toivonen & E. Saari (Éds.), Human-Centered Digitalization and Services (p. 101-118). Springer Nature. https://doi.org/10.1007/978-981-13-7725-9_6

Ross, A., Banerjee, S., & Chowdhury, A. (2022). Deducing health cues from biometric data. Computer Vision and Image Understanding, 221, 103438. https://doi.org/10.1016/j.cviu.2022.103438

Roth, T., Rieger, A., & Hoess, A. (2024). From Mutualism to Amensalism : A Case Study of Blockchain and Digital Identity Wallets. In B. Shishkov (Éd.), Business Modeling and Software Design (p. 149-165). Springer Nature Switzerland.

Sarkis, J., Koo, C., & Watson, R. T. (2013). Green information systems & technologies – this generation and beyond : Introduction to the special issue. Information Systems Frontiers, 15(5), 695-704. https://doi.org/10.1007/s10796-013-9454-5

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. ECIS 2022 Research Papers. https://aisel.aisnet.org/ecis2022_rp/46

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. Information & Management, 103553. https://doi.org/10.1016/j.im.2021.103553

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2021). Identity at the margins : Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. Information Technology for Development, 27(1), 13-36. https://doi.org/10.1080/02681102.2020.1785826

Schoemaker, E., Martin, A., & Weitzberg, K. (2023). Digital Identity and Inclusion : Tracing Technological Transitions. Georgetown Journal of International Affairs, 24(1), 36-45. https://doi.org/10.1353/gia.2023.a897699

Secure Identity Alliance. (2019). Putting government back in control—Solving vendor lock-in with open standards. https://www.id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology : Beyond Myth. Business & Information Systems Engineering, 62(6), 599-608. https://doi.org/10.1007/s12599-020-00656-x

Sedlmeir, J., Huber, J., Barbereau, T., Weigl, L., & Roth, T. (2022). Transition Pathways towards Design Principles of Self-Sovereign Identity.

Sedlmeir, J., Rieger, A., Roth, T., & Fridgen, G. (2023). Battling disinformation with cryptography. Nature Machine Intelligence, 5. https://doi.org/10.1038/s42256-023-00733-2

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. Business & Information Systems Engineering, 63(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Seidel, S., Bharati, P., Fridgen, G., Watson, R., Albizri, A., Boudreau, M.-C., Butler, T., Chandra Kruse, L., Guzman, I., Karsten, H., Lee, H., Melville, N., Rush, D., Toland, J., & Watts, S. (2017). The Sustainability Imperative in Information Systems Research. Communications of the Association for Information Systems, 40. https://doi.org/10.17705/1CAIS.04003

Shirlow, P. (2021). Lustration in Iraq : Regime change as exclusion and control. Capital & Class, 45(1), 123-144. https://doi.org/10.1177/0309816820924400

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management : The Implications to Personal Data Protection. 2019 IEEE Conference on Application, Information and Network Security (AINS), 30-35. https://doi.org/10.1109/AINS47559.2019.8968708

Smethurst, R. (2023). Digital Identity Wallets and their Semantic Contradictions. Thirty-First European Conference on Information Systems. https://aisel.aisnet.org/ecis2023_rp/288

Spulbar, C., Anghel, L. C., Birau, R., Ermiș, S. I., Treapăt, L.-M., & Mitroi, A. T. (2022). Digitalization as a Factor in Reducing Poverty and Its Implications in the Context of the COVID-19 Pandemic. Sustainability, 14(17), Article 17. https://doi.org/10.3390/su141710667

Sridhar, S., Altinkemer, K., & Rees, J. (2005). Software Vulnerabilities : Open Source versus Proprietary Software Security.

Stoker, G. (2006). Public Value Management : A New Narrative for Networked Governance? The American Review of Public Administration, 36(1), 41-57. https://doi.org/10.1177/0275074005282583

Swiss Federal Counsel. (2021). Arrêté du Conseil fédéral constatant le résultat de la votation populaire du 7 mars 2021. https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2021/1185/de/pdf-a/fedlex-data-admin-ch-eli-fga-2021-1185-de-pdf-a.pdf

Swiss Federal Counsel. (2023). E-ID : adoption du message par le Conseil fédéral. https://www.bj.admin.ch/bj/fr/home/aktuell/mm.msg-id-98758.html

Tavares, A. P., & Masiero, S. (2023). Digital Identity and Social Protection Programs : Leaving No One Behind?

Taylor, J. A., Lips, M., & Organ, J. (2008). Identification practices in government : Citizen surveillance and the quest for public service improvement. Identity in the Information Society, 1(1), 135-154. https://doi.org/10.1007/s12394-009-0007-5

The Alan Turing Institute. (2021). Openness in the digital identity context. The Alan Turing Institute. https://www.turing.ac.uk/programme/openness-digital-identity-context

Thomas, S. (1998). User fees, self-selection and the poor in Bangladesh. Health Policy and Planning, 13(1), 50-58. https://doi.org/10.1093/heapol/13.1.50

Tiwari, K., & Gupta, P. (2014). Fingerprint Quality of Rural Population and Impact of Multiple Scanners on Recognition. In Z. Sun, S. Shan, H. Sang, J. Zhou, Y. Wang, & W. Yuan (Éds.), Biometric Recognition (p. 199-207). Springer International Publishing. https://doi.org/10.1007/978-3-319-12484-1_22

UIDAI. (2022). Training, Testing & Certification Ecosystem. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/ecosystem/training-testing-certification-ecosystem.html

UIDAI. (2023). Enrolment Agencies. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/ecosystem/enrolment-ecosystem/enrolment-agencies.html

UNCDF. (2020, décembre). RFA Feasibility Study for setting up a single identification system for financial service users in the WAEMU (UEMOA).

UNDP. (2023). The DPI approach, a playbook. https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-the-dpi-approach-a-playbook.pdf

UNHCR. (2018). UNHCR Strategy on Digital Identity and Inclusion.

USAID. (2017). Identity in a Digital Age : Infrastructure for Inclusive Development. https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf

van der Wal, Z., & van Hout, E. Th. J. (2009). Is Public Value Pluralism Paramount? The Intrinsic Multiplicity and Hybridity of Public Values. International Journal of Public Administration, 32(3-4), 220-231. https://doi.org/10.1080/01900690902732681

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. New Media & Society, 22(5), 896-914. https://doi.org/10.1177/1461444819872537

Verheul, E., & Jacobs, B. (2017). Polymorphic encryption and pseudonymisation in identity management and medical research.

Veseli, F., Olvera, J. S., Pulls, T., & Rannenberg, K. (2019). Engineering privacy by design : Lessons from the design and implementation of an identity wallet platform. Proceedings of the

34th ACM/SIGAPP Symposium on Applied Computing, 1475-1483. https://doi.org/10.1145/3297280.3297429

W3C. (2022). Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/

Wachter, S., & Mittelstadt, B. (2018). A Right to Reasonable Inferences : Re-Thinking Data Protection Law in the Age of Big Data and AI (SSRN Scholarly Paper No. 3248829). https://papers.ssrn.com/abstract=3248829

Walker, R. M., Brewer, G. A., Boyne, G. A., & Avellaneda, C. N. (2011). Market Orientation and Public Service Performance : New Public Management Gone Mad? Public Administration Review, 71(5), 707-717. https://doi.org/10.1111/j.1540-6210.2011.02410.x

Walton, R. (2016). Supporting Human Dignity and Human Rights : A Call to Adopt the First Principle of Human-Centered Design. Journal of Technical Writing and Communication, 46(4), 402-426. https://doi.org/10.1177/0047281616653496

Wang, F., & Filippi, P. (2020). Self-Sovereign Identity in a Globalized World : Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, 2, 28. https://doi.org/10.3389/fbloc.2019.00028

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. Electronic Markets, 12(3), 157-162. https://doi.org/10.1080/101967802320245929

Watling, S. (2011). Digital exclusion : Coming out from behind closed doors. Disability & Society, 26(4), 491-495. https://doi.org/10.1080/09687599.2011.567802

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU's Digital Identity Policy : Tracing Policy Punctuations. 15th International Conference on Theory and Practice of Electronic Governance, 74-81. https://doi.org/10.1145/3560107.3560121

Weigl, L., Amard, A., Marxen, H., Roth, T., & Zavolokina, L. (2022). User-centricity and Public Values in eGovernment : Friend or Foe?

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of Self-Sovereign Identity : Extending the interpretive flexibility of technology towards institutions. Government Information Quarterly, 40(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Weigl, L., Barbereau, T. J., Rieger, A., & Fridgen, G. (2022a). The Social Construction of Self-Sovereign Identity : An Extended Model of Interpretive Flexibility. Proceedings of the 55th Hawaii International Conference on System Sciences, 2543-2552.

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022b). The Social Construction of Self-Sovereign Identity : An Extended Model of Interpretive Flexibility. Proceedings of the Hawaii International Conference on System Sciences 2022, 2543-2552.

Weigl, L., Roth, T., Amard, A., & Zavolokina, L. (2024). When public values and user-centricity in e-government collide—A systematic review. Government Information Quarterly. https://doi.org/10.1016/j.giq.2024.101956

Welch, E. W., Hinnant, C. C., & Jae, M. M. (2004). Linking Citizen Satisfaction with E-Government and Trust in Government. Journal of Public Administration Research and Theory, 15(3), 371-391. https://doi.org/10.1093/jopart/mui021

Wickins, J. (2007). The ethics of biometrics : The risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics, 13(1), 45-54. https://doi.org/10.1007/s11948-007-9003-z

Williams, D. (2000). Aid and sovereignty : Quasi-states and the international financial institutions. Review of International Studies, 26(4), 557-573. https://doi.org/10.1017/S026021050000557X

Witten, B., Landwehr, C., & Caloyannides, M. (2001). Does open source improve system security? IEEE Software, 18(5), 57-61. IEEE Software. https://doi.org/10.1109/52.951496

Woo, J., & Kumar, M. S. (2015). Public Debt and Growth. Economica, 82(328), 705-739. https://doi.org/10.1111/ecca.12138

World Bank. (2014). Digital Identity Toolkit. https://openknowledge.worldbank.org/server/api/core/bitstreams/ec566c87-09c4-5171-ab8d-9f3707c613f0/content

World Bank. (2018). International Development Association project appraisal document on a proposed credits and grant to the republic of Côte d'Ivoire & the Republic of Guinea. https://documents1.worldbank.org/curated/en/771571528428669934/pdf/REGIONAL-INTEGRATION-CAS-AFRICArev-05152018.pdf

World Bank. (2019a). ID4D Practitioner’s Guide.pdf. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

World Bank. (2019b). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World’s Most Vulnerable. World Bank. https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

World Bank. (2019c). Procurement-Guide-And-Checklist-For-Digital-Identification-Systems.pdf. https://documents1.worldbank.org/curated/en/104171583178428889/pdf/Procurement-Guide-And-Checklist-For-Digital-Identification-Systems.pdf

World Bank. (2022). Identification for Development (ID4D) and Digitalizing G2P Payments (G2Px) 2022 Annual Report [Text/HTML]. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099437402012317995/IDU00fd54093061a70475b0a3b50dd7e6cdfe147

World Bank. (2023a). The West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program : Unique Identifiers to Enable Access to Human Development Services. Washington, DC: World Bank. https://doi.org/10.1596/40121

World Bank. (2023b, mars 15). How digital public infrastructure supports empowerment, inclusion, and resilience. https://blogs.worldbank.org/digital-development/how-digital-public-infrastructure-supports-empowerment-inclusion-and-resilience

Yang, L., Hu, L., & Li, Y. (2024). Institutional Environment, Institutional Arrangements, and Risk Identification and Allocation in Public–Private Partnerships : A Multilevel Model Analysis Based on Data from 31 Provinces in China. Sustainability, 16(15), Article 15. https://doi.org/10.3390/su16156674

Zavolokina, L., Sprenkamp, K., & Schenk, B. (2023). Citizens’ Expectations about Achieving Public Value and the Role of Digital Technologies : It Takes Three to Tango! https://doi.org/10.24251/HICSS.2023.243

Zdjelar, R., & Žajdela Hrustek, N. (2021). Digital Divide and E-Inclusion as Challenges of the Information Society – Research Review. Journal of Information and Organizational Sciences, 45(2), 601-638. https://doi.org/10.31341/jios.45.2.14

Appendix

1 Publication Portfolio

A.1 Publications included in this thesis

RP1: Amard, A., Hartwich, E., Höß, A., Rieger, A., Roth, T., & Fridgen, G. (2024). Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://scholarspace.manoa.hawaii.edu/items/27f184ba-959e-4bf3-9134-5e3a7506e7ed

Conference Ranking: 2 (GGS Class); A (GGS Rating)

RP2: Amard, A., Frigden, G. (Forthcoming). Challenges in designing digital identity infrastructure for development: A taxonomy of strategic institutional and governance choices. *Information Technology for Development. Under revision.*

Journal Ranking: 97% Public Administration; Journal Rating: 11.3 (CiteScore); 5.1 (Impact Factor)

RP3: Weigl, L., Amard, A., Fridgen, G., Codagnone, C. (2022). The EU's Digital Identity Policy: Tracing Policy Punctuations. In *15th International Conference on Theory and Practice of Electronic Governance*. https://doi.org/10.1145/3560107.3560121

Conference Ranking: Work in Progress (GGS Class); Work in Progress (GGS Rating)

RP4: Weigl, L., Amard, A., Marxen, H., Roth, T., Zavolokina, L. (2022). User-centricity and Public Values in eGovernment: Friend or Foe? In 30th European Conference on Information Systems. 15. https://aisel.aisnet.org/ecis2022_rp/15

Conference Ranking: 2 (GGS Class); B (GGS Rating)

RP5: Weigl, L., Amard, A., Roth, T., Zavolokina, L. (2023). When Public Values and User-Centricity in eGovernment Collide – a Systematic Review. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2024.101956

Journal Ranking: 99% Law, Sociology and Political Science; Journal Rating: 15.7 (CiteScore); 7.8 (Impact Factor)

RP6: Amard, A., Höß, A., Roth, T., Fridgen, G., & Rieger, A. (2022). Guiding Refugees Through European Bureaucracy: Designing a Trustworthy Mobile App for Document Management. In *The Transdisciplinary Reach of Design Science Research. DESRIST 2022* (pp. 171–182). https://doi.org/10.1007/978-3-031-06516-3_13

Conference Ranking: Work in Progress (GGS Class); Work in Progress (GGS Rating)

BC1: Amard, A., Hölzmer, P., Hoess, A. (2024). Decentralized Digital Identities. In: Fridgen, G., Guggenberger, T., Sedlmeir, J., Urbach, N. (eds) Decentralization Technologies. Financial Innovation and Technology. Springer, Cham. https://doi.org/10.1007/978-3-031-66047-4_4

A.2 Publications not included in this thesis

Amard, A., Delgado Fernandez, J., Barbereau, T. J., Fridgen, G., & Sedlmeir, J. (2023). *Federated Learning in Migration Forecasting* [Paper presentation]. ICIS 2023.

https://aisel.aisnet.org/treos_icis2023/23/

Conference Ranking: 2 (GGS Class); A- (GGS Rating)

2 Author Contribution Statements

The following pages outline the individual contribution of all co-authors to the research papers included in this thesis, using the roles introduced by ANSI/NISO Z39.104-2022, CRediT, Contributor Roles Taxonomy.

RP1: Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices

- **Alexandre Amard – Primary Author**: Conceptualization, Validation, Investigation, Data Curation, Writing – Original Draft, Visualization, Project Administration.
- **Gilbert Fridgen – Non-primary Author**: Writing – Review & Editing, Supervision, Funding Acquisition.
- **Eduard Hartwich – Non-primary Author**: Conceptualization, Methodology, Writing – Original Draft, Writing – Review & Editing.
- **Alexandra Hoess – Non-primary Author**: Conceptualization, Investigation, Methodology, Writing – Review & Editing.
- **Alexander Rieger – Non-primary Author**: Conceptualization, Writing – Review & Editing, Supervision.

- **Tamara Roth – Non-primary Author**: Conceptualization, Writing – Review & Editing, Investigation, Supervision.

RP2: Challenges in designing digital identity infrastructure for development: A taxonomy of strategic institutional and governance choices

- **Alexandre Amard – Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Writing – Original Draft, Visualization, Project Administration.
- **Gilbert Fridgen – Non-primary Author**: Writing – Review & Editing, Supervision, Funding Acquisition.

RP3: The EU's Digital Identity Policy: Tracing Policy Punctuations

- **Alexandre Amard – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Visualization, Writing – Original Draft, Writing – Review & Editing, Project Administration.
- **Cristiano Codagnone – Non-primary Author**: Writing – Review & Editing, Supervision, Funding Acquisition.
- **Gilbert Fridgen – Non-primary Author**: Writing – Review & Editing, Supervision, Funding Acquisition.
- **Linda Weigl – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Visualization, Writing – Original Draft, Writing – Review & Editing, Project Administration.

RP4: User-centricity and Public Values in eGovernment: Friend or Foe?

- **Alexandre Amard – Non-primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Visualization, Writing – Review & Editing.
- **Hanna Marxen – Non-primary Author**: Validation, Investigation, Data Curation.
- **Tamara Roth – Non-primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Writing – Review & Editing.
- **Linda Weigl – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Writing – Original Draft, Visualization, Project Administration, Writing – Review & Editing, Supervision, Funding Acquisition.
- **Liudmila Zavolokina – Non-primary Author**: Conceptualization, Methodology, Writing – Review & Editing, Supervision, Funding Acquisition.

RP5: When Public Values and User-Centricity in e-Government Collide – a Systematic Review

- **Alexandre Amard – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Visualization, Writing – Review & Editing.
- **Tamara Roth – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Writing – Review & Editing.
- **Linda Weigl – Joint Primary Author**: Conceptualization, Methodology, Validation, Investigation, Data Curation, Writing – Original Draft, Visualization, Project Administration, Writing – Review & Editing, Supervision, Funding Acquisition.
- **Liudmila Zavolokina – Non-primary Author**: Conceptualization, Methodology, Writing – Review & Editing, Supervision, Funding Acquisition.

RP6: Guiding Refugees Through European Bureaucracy: Designing a Trustworthy Mobile App for Document Management

- **Alexandre Amard – Joint Primary Author**: Conceptualization, Writing – Review & Editing.
- **Alexandra Hoess – Joint Primary Author**: Investigation, Methodology, Writing - Original Draft, Writing – Review & Editing, Visualization.
- **Tamara Roth – Joint Primary Author**: Conceptualization, Investigation, Methodology, Visualization, Validation, Writing – Original draft, Writing – Review & Editing, Project Administration.
- **Gilbert Fridgen – Non-primary Author**: Writing - Review & Editing, Funding Acquisition.
- **Alexander Rieger – Non-primary Author**: Writing - Review & Editing.

BC1: Decentralized Digital Identities

- **Alexandre Amard – Joint Primary Author**: Conceptualization, Writing - Original Draft, Writing – Review & Editing, Project Administration.
- **Pol Hölzmer – Joint Primary Author**: Conceptualization, Writing - Original Draft, Writing – Review & Editing, Visualization, Project Administration.
- **Alexandra Hoess – Joint Primary Author**: Conceptualization, Writing - Original Draft, Writing – Review & Editing, Project Administration.

3 Appended Research Papers

Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices

Alexandre Amard
University of Luxembourg
Alexandre.amard@uni.lu

Eduard Hartwich
University of Luxembourg
Eduard.hartwich@uni.lu

Alexandra Hoess
University of Luxembourg
Alexandra.hoess@uni.lu

Alexander Rieger
University of Luxembourg
Alexander.rieger@uni.lu

Tamara Roth
University of Luxembourg
Tamara.roth@uni.lu

Gilbert Fridgen
University of Luxembourg
Gilbert.fridgen@uni.lu

Abstract

Governments around the world increasingly deploy digital identity infrastructure. These initiatives are considered a fundamental building block for their citizens to reap the benefits of digitalization and take part in the digital society and economy. But this outcome is not guaranteed: it considerably hinges upon a range of strategic governance decision domains that institutional actors must act on when designing digital identity infrastructures. To get a better understanding of how governments can approach this critical design aspect, we propose a taxonomy of strategic governance choices for digital identity infrastructures. This taxonomy is the outcome of an analysis of 13 government-led digital identity infrastructures and 12 expert interviews. This paper contributes to the digital government literature by setting a foundation for further research and theory-building on digital identity infrastructure. Practitioners can use the taxonomy to develop governance strategies for their own digital identity infrastructure.

Keywords: Digital identity, digital infrastructure, digital government, eGovernment, governance.

1. Introduction

Digital identity infrastructure is deemed essential for the effective provision of society-wide functions and services provided by the government or private sector (Henfridsson & Bygstad, 2013; DPGA & GiZ, 2022). It is credited with a capacity to support socio-economic development (Addo & Senyo, 2021; Masiero & Bailur, 2021), enable individual agency (Whitley & Schoemaker, 2022), improve social inclusion (Wang & Filippi, 2020) and is commonly viewed as an integral component to reach sustainable development as reflected through the United Nations' Sustainable Development Goal 16.9 "Legal identity for all, including birth registration, by 2030" (UN Legal Identity Expert Group, 2019). It is expected that digital identity systems could "unlock value equivalent to 3 to 13 percent of GDP by 2030" (McKinsey, 2019). In light of these asserted benefits, the development of reliable digital identity infrastructure has become a high priority for governments to enable their citizens to take full advantage of the opportunities that digitalization represents (Gelb & Diofasi, 2018), and a number of countries around the world have built their own digital identity infrastructures, including India, Nigeria, Peru, Singapore and most European countries. Many more commit substantial resources to build or improve their own digital identity capabilities (World Bank, 2022b).

Yet, not all digital identity infrastructure is successful in realizing these benefits (Walke et al., 2023). Many recent initiatives have exhibited varying signs of failure, ranging from low adoption to outright discontinuation, or even citizen rejection prior to implementation. A 2021 PwC survey revealed that Germany's electronic identification scheme had a very low uptake, with only 7% of citizens having used their electronic identity document in 11 years following its introduction (PwC, 2021). In the UK, the GOV.UK Verify infrastructure, that was expected to be taken over by the private sector by 2020, was publicly qualified as a failure (National Audit Office, 2019) and fully discontinued in 2023, a few months after the UK's taxation authority withdrew from the scheme. The total cost for the infrastructure was estimated to be £220m. In Switzerland, the digital identity infrastructure did not even get a chance to start: in March 2021, a referendum saw the adoption of the Electronic Identification Services Act overwhelmingly rejected. This failure was largely attributed to the role that the private sector would have taken in provisioning digital identities. Again in 2021, the Comptroller and Auditor General of India heavily criticized the Unique Identification Authority of

URI: https://hdl.handle.net/10125/106646
978-0-9981331-7-1

India's (UIDAI) national digital identity infrastructure Aadhar, not least because of the poorly established relationship between government and private sector partners (CAG of India, 2021). To build and manage its identity infrastructure, the UIDAI spent Rs 15764.48 Crore (~$1.8bn) from its inception in 2009 until February 2023 (UIDAI, 2023).

In all these cases, failures were widely attributed to strategic design choices made regarding *governance*; conceptualized in this paper as the macro-level choices happening at the intersection between relational governance, corporate governance and infrastructure governance (Saunders et al., 2020). These failures caused public distrust and waste of public resources to replace the positive outcomes that had been expected from the infrastructure. The importance of governance arrangements has long been established, and their mechanisms studied extensively. Public-private links, service diversity, user awareness and acceptance, regulation and organizational structures are governance-related factors that can influence the success of digital identity infrastructure (Walke et al., 2023). Additionally, both organizational and institutional arrangements impact the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), reinforcing their central role in realizing the infrastructure's value.

This challenge is compounded by the fact that institutional actors are confronted with a myriad of governance design options for digital identity infrastructure. These choices will impact the infrastructure, the services that rely on it and its users for years, if not decades.

A detailed look at instantiations around the world reveals wildly different implementations and substantial design complexity. For example, in Scandinavian countries, banks play a crucial role in providing digital identity services to citizens who use their 'BankID' on a daily basis for various identification purposes. On the other hand, some countries such as Spain have built their digital identity capabilities around public sector needs, and the private sector is primarily acting as a subcontractor. The Indian Aadhar system is led by the public sector, with extensive participation of the private sector, including for the enrolment of citizens. These are just a few of the existing governance configurations in an area where disruptive technologies are increasingly deployed. Then, how can institutional actors have confidence that they evaluated the most important governance design options? What are the governance choices available to them that will have substantial impact on the design and ultimate success of the costly infrastructure? Despite their criticality, so far, no consolidated answer to these questions has been offered. While some of the topics at hand are individually addressed in the literature, to our knowledge, there is no systematic guidance and terminology on the strategic governance choices for digital identity infrastructure. In response, we formulate the following research question:

Research Question: *What are the strategic governance choices impacting the design of digital identity infrastructure?*

We answer this research question by developing a multi-layer taxonomy for the governance of digital identity infrastructure. Our development process follows Nickerson et al. (2013) and involved 4 iterations, which included (1) a literature review, (2) interviews with practitioners and (3) with researchers in the field of digital identity infrastructures, and (4) an analysis of governance models of existing digital identity systems. Our final taxonomy consists of three layers, 13 dimensions and 46 characteristics. It establishes a holistic overview of the critical governance decisions required during the design of digital identity infrastructure and consolidates terminology to facilitate collaboration during this process.

This paper is structured as follows. In Section 2, we present the theoretical background regarding digital identity and digital identity infrastructure. We then discuss the implementation of our research method in Section 3, which we used to develop a multi-layer taxonomy presented in Section 4. Finally, in Section 5, we reflect on our findings, acknowledging their implications and limitations, and propose avenues for future research.

2. Theoretical Background

2.1. Digital identity

In this article, we conceptualize *digital identity* as the set of digitalized identity attributes and credentials that describe qualities, characteristics, or assertions of a person (Temoshok et al., 2022). This set of attributes and credentials can be used for the identification and authentication of a person via digital channels, for instance, to provide governmental and private sector services (Nyst et al., 2016). Digital credentials are the means through which a subject can assert their digital identity (Sedlmeir et al., 2021). These credentials can take several forms, ranging from electronic identity documents to smartphone-stored digital documents, and are sometimes enhanced with other authentication factors such as biometrics or passwords to allow for a higher level of authentication assurance (World Bank, 2019a). A digital credential can also simply be a reference to a digital record in a database, or directly contain identity attributes. Cryptographic methods are employed to ensure the integrity and authenticity of credentials (Sedlmeir et al., 2021), while safeguards and controls are used to support data protection and prevent data leakage and identity theft (McCallister et al., 2010).

Digital identity emanates from entities in charge of collecting and verifying identity data about a subject and translating it into the digital realm. As digital identity is not a monolithic construct, identity data and credentials making up a digital identity can be collected, stored, certified, and issued by different stakeholders (Grassi et al., 2017). These authoritative entities hold data that is accepted as accurate and trustworthy within a particular sector of application (e.g., taxation, criminal records, and health). In many countries, linkability of identity data (e.g., through unique identifiers or mediating entities), which allows for the re-identification of a data subject in different circumstances, is strictly regulated for privacy and data protection purposes (Beduschi, 2019). The capacity to materialize the benefits of digital identity, including the capacity to collect, store and verify identity attributes, enroll and authenticate users, and manage credentials and authorizations, requires the establishment of a digital identity infrastructure (Nyst et al., 2016).

2.2. Digital identity infrastructure

Digital infrastructure refers to digital, socio-technical systems that underlie or support the public interest, as well as universal or quasi-universal services (Plantin et al., 2018). The notion of digital infrastructure conceptualizes the reality of interconnected system collectives, which evolve at the intersection between socio-technical elements, networks of actors and relationships between organized practices (Henfridsson & Bygstad, 2013). Thus, the study on digital infrastructure extends beyond the historic information systems focus, being shared, unbounded, heterogenous and evolving (Hanseth & Lyytinen, 2010). Digital infrastructure (also sometimes called *digital public infrastructure* by practitioners (DPGA & GiZ, 2022)) applies within a society-wide, public service-oriented context, including for digital identity management systems (Boysen, 2019).

Digital identity infrastructures can be defined as systems that construct, control, and commodify (facets of) digital identities and can be formed by both public and private sector actors (Giannopoulou, 2023). Despite many having a national dimension, some digital identity infrastructures target transnational interoperability (e.g., the West Africa Unique Identification for Regional Integration program, or the electronic Identification, Authentication and Trust Services regulation). Others, in turn, operate at the sub-national level (e.g., the Ontario and Alberta provinces). Digital identity infrastructures are credited with various potential benefits, ranging from the “facilitat[ion] and simplif[ication of] access to a wide range of services and thereby contribute to social and economic value” (OECD, 2023), better “inclusion, social protection, healthcare and education, gender equality, child protection”, “delivery of public services and programs”, and the “reduction of fraud” (World Bank, 2019b). On the other hand, implementation of these systems can also cause adverse impacts, such as “exclusion from access”, “distortion of monitoring”, “redirection of policy” (Masiero & Arvidsson, 2021), “privacy and security violations” among others (Beduschi, 2019; World Bank, 2019a).

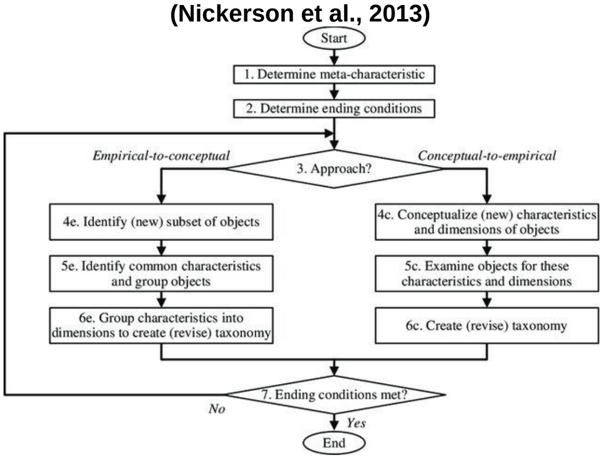
Digital identity infrastructures are to be considered within the complex socio-technical systems that structure them (van Dijck & Jacobs, 2020; Weigl, Barbereau, et al., 2022). It is well-established that organizational and institutional arrangements significantly influence the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), thus playing an important role in the design of digital infrastructure. It follows that considering actors, roles, people and processes is a necessary condition for the development and implementation of useful and sustainable infrastructures (Dawes, 2009; Manny et al., 2022). Digital identity infrastructure design and success are therefore inextricably interlocked with the strategic governance choices that impact them (Gil-Garcia & Flores-Zúñiga, 2020; Medaglia et al., 2022), and their identification and characterization should be a priority.

3. Research method

Given the nascent nature and rapid development of digital identity infrastructures, we opted to develop a taxonomy (Bailey, 1994) to understand, classify and systematically structure common characteristics of strategic governance choices when designing digital identity infrastructure. Taxonomies are common means to this end, and they are frequently used across information systems research (Berger et al., 2020; Hartwich et al., 2022). Further, taxonomies can serve as a foundation upon which research and practice can build: as such, we address information systems scholars, policymakers and practitioners in the field of e-government.

In order to develop our taxonomy, we structure our approach following the method outlined by Nickerson et al. (2013). This iterative process, as illustrated in Figure 1, consists of seven steps which are considered completed once defined ending conditions are met. We rigorously followed this process to ensure reproducibility of our results.

Figure 1. Taxonomy development method (Nickerson et al., 2013)


Start
1. Determine meta-characteristic
2. Determine ending conditions
Empirical-to-conceptual
3. Approach?
Conceptual-to-empirical
4e. Identify (new) subset of objects
4c. Conceptualize (new) characteristics and dimensions of objects
5e. Identify common characteristics and group objects
5c. Examine objects for these characteristics and dimensions
6e. Group characteristics into dimensions to create (revise) taxonomy
6c. Create (revise) taxonomy
7. Ending conditions met?
No
Yes
End

3.1. Taxonomy development process

Our purpose is to systematically classify the dimensions and characteristics of governance-related decision domains that are key for the design of digital identity infrastructures. We thus selected our meta-characteristic to be "Strategic Governance Choices for Digital Identity Infrastructure". We then determined our objective and subjective ending conditions. Objective ending conditions target the formal aspects of taxonomy building and indicate that the taxonomy building process and its iterations can be concluded once they are met (Nickerson et al., 2013). Subjective ending conditions play an important role as they relate to the usefulness of the taxonomy's content. We set out to validate every objective ending conditions as outlined by Nickerson et al. (2013). These can be broadly classified into 3 categories: (1) the last iteration should not have induced any needed change in the taxonomy, (2) there should be no repetition or duplication between dimensions and characteristics, and there should only be dimensions or characteristics that represent at least one object under analysis, and (3) all objects, or a representative sample thereof, have been analyzed.

These conditions were tested at the end of each iteration, and we devoted the last iteration to specifically analyze a representative sample of objects. An exhaustive analysis of all existing digital identity infrastructures is not feasible, not only because of the important number of instantiations in existence, but also because they evolve rapidly, and limited information is readily available for many of them. We thus selected a sample of 13 instantiations that are widely referred to as archetypes for specific dimensions of digital identity infrastructure governance and thus influenced the governance models of other instantiations: Argentina, Australia, Canada, Chile, Estonia, France, Germany, India, Italy, Morocco, Nigeria, Sweden, United Kingdom. These present particularly interesting and salient characteristics, and their geographical coverage is varied.

As regards subjective ending conditions, we requested an assessment of our taxonomy's usefulness, robustness (i.e., does it enable sufficient differentiation between objects to be of interest), and explanatory character from our interview partners, who would later use this taxonomy in their work and thus are the best placed to provide feedback.

3.2. Iterations

We needed four iterations to meet the ending conditions and reach the final version of the taxonomy. Our first iteration took a conceptual to empirical approach and built on existing academic and practitioner-sourced material dealing with classification of digital identity management systems. We searched the existing body of academic and grey literature dealing with governance of digital identity infrastructure, using the search string "digital identity governance" OR "digital identity infrastructure" OR "digital infrastructure governance". This initial phase was primarily used to identify works of relevance for a second stage of backward and forward searching that allowed us to identify the most relevant work in this area. After screening for eligibility, this process yielded 65 articles and documents, 32 from academic literature and 33 from grey literature. The work of the National Institute of Science and Technology (Grassi et al., 2017), the International Telecommunication Union (ITU, 2018) and the World Bank (World Bank, 2014, 2022a, 2019a) were particularly useful during this iteration. It laid down the foundations of the taxonomy, with the three layers of *ecosystem governance*, *IT governance* and *data governance* emerging. We could additionally identify several dimensions and characteristics that would remain until the final version of the taxonomy. In total, nine dimensions and 28 characteristics were identified. This iteration confirmed that while some useful knowledge supporting the answering of our research question had been synthesized, content was spread out and the vocabulary used varied significantly.

The second iteration took an empirical to conceptual approach and consisted in the interview of eight practitioners. They were selected for their expertise and experience (Mergel et al., 2019) in the design of governance arrangements of digital identity systems. The interviewees came from both the public and the private sector, and the semi-structured interviews (Schultze & Avital, 2011) lasted between 30 and 90 minutes. Several participants had been involved in the design of multiple digital identity infrastructures, which enabled them to adopt a global, synthetic perspective. This iteration enabled us to both expand the taxonomy and refine it towards meeting our subjective ending conditions. In total, we identified 12 dimensions and 47 characteristics. Towards the end of the iteration, we noticed that we approached theoretical saturation as no new dimensions or characteristics were being identified. All of the interview participants were explicitly asked about the usefulness subjective ending condition, and all agreed that the taxonomy was meeting this criterion. The robustness and explanatory character were evaluated through their intuitive understanding of the taxonomy, and their capacity to easily distinguish between the characteristics identified.

To ensure rigor, we conducted a third iteration with an empirical to conceptual approach, that consisted in the interview of four researchers with high expertise in the field of digital identity infrastructure and e-government. These semi-structured interviews also lasted between 30 and 90 minutes. Aside from bringing back a previously dismissed dimension and clarifying some of the vocabulary, this iteration did not yield any substantial changes to the taxonomy, thus confirming theoretical saturation. This iteration mainly supported us in improving the comprehensiveness, conciseness and explanatory character of the taxonomy (Nickerson et al., 2013). In total, 13 dimensions and 46 characteristics were retained. Subjective ending conditions were assessed in the same way as in the previous iteration, with the same outcome.

Finally, to validate our final ending condition, i.e., the adequate representation of a representative sample of objects, we proceeded with an empirical to conceptual approach, analyzing instantiations of 13 digital identity infrastructures. This iteration did not yield any further change compared to the previous iteration. The fact that, on the basis of the information available to us at the time of writing, all objects fit within our taxonomy and all characteristics were used, confirmed that we had met all the ending conditions and could conclude the taxonomy development process.

4. Taxonomy of digital identity infrastructures

The following section presents the taxonomy as an outcome of the four iterations of our taxonomy building process. It includes three layers, 13 dimensions, 46 characteristics. Except for the first dimension (ID authority governance model), none of the characteristics are mutually exclusive, meaning that a combination thereof is possible. In the following, we illustratively refer to instantiations that we analyzed during the last iteration of the taxonomy development process.

4.1. Ecosystem management layer

The ecosystem management layer is composed of five dimensions: **orchestrating authority**, **scope**, **cross-ecosystem interoperability**, **subjects**, and **roles of private sector actors**.

Orchestrating authority (mutually exclusive): describes how the authority responsible for setting policies and standards, certifying partners and supervising implementation (e.g., the UIDAI in India), is governed. This can take the following forms. *Inter-ministerial entity*: an arrangement in which the authority is shared as part of an inter-ministerial delegation (e.g., France). *Ministerial entity*: the authority is given to an entity within an existing ministry (e.g., the Ministry of Interior and Transportation in Argentina). *Autonomous entity with ministerial board representation*: the authority is given autonomy from a ministry, but the governing board has governmental stakeholder representation (e.g., Nigeria). *Fully autonomous entity*: the authority is autonomous and is only reporting to the highest levels of government (e.g., India).

Scope: describes how the system relates to the sovereign state. It can be *sub-national* (e.g., a region, state or territory), which is typical in federal states such as Canada or Australia. These might have an additional interoperability layer at the national level. *National* systems are common in non-federal states, such as Peru or Morocco. The *transnational* characteristic highlights that some systems are meant to be usable across borders, as is the case for eIDAS in Europe or WURI in Africa.

Interoperability approach: defines if and how interoperability with other systems is approached. It can be the case that *no interoperability* is foreseen. While some digital identity systems do not foresee interoperability with other systems, we identified several digital identity systems that are interoperable with one another (e.g., eIDAS-notified identity schemes).

	Layer	Dimension	Characteristics						
Strategic Governance Choices for Digital Identity Infrastructure	Ecosystem Management	**Orchestrating authority**	Inter-ministerial entity	Ministerial entity	Autonomous entity with ministerial board representation	Fully autonomous entity			
		Scope	Sub-national	National	Transnational				
		Interoperability approach	None	Harmonization	Mutual recognition				
		Subjects	Resident nationals	Non-resident nationals	Resident non-nationals	Non-resident non-nationals	Domestic juridical persons	Foreign juridical persons	Persons without proof of legal identity
		Roles of private sector actors	None	Authoritative source	Registrar	Data manager	Credential provider	Trust and orchestration service provider	Relying party
	IT Management	**Operation and ownership**	Public infrastructure	Private infrastructure					
		Software licensing	Closed source	Open source					
		Standards usage	Compliant	Non-compliant					
		Development funding	Public	Grant	Private				
		Operational financing	Public budget	Charge for identity providers	Charge for relying parties	Charge for data subjects			
	Data Management	**Exchange model**	Identity provider to relying party	Data subject to relying party	Federation through 1 actor	Federation through multiple actors			
		Linkability	Mediated	Non-mediated					
		Trusted data storage	Cross-sectoral repositories	Sectoral repositories	User wallets				

Table 1. Final taxonomy of strategic governance choices for digital identity infrastructures.

One approach to achieve such interoperability is *mutual recognition*, meaning that while there might be discrepancies between the rules and procedures of the digital identity system, a state could still accept to recognize digital identities issued by another state (Davies, 2006), as is the case for eIDAS in its current state. *Harmonization* goes one step further and mandates the implementation of a similar set of rules and procedures (e.g., digital wallets within the upcoming European Digital Identity Framework (Weigl, Amard, et al., 2022)).

Subjects: different categories of subjects can be included in the digital identity system. *Resident nationals* are often the primary target group, but *non-resident nationals* and *resident non-nationals* are also often considered as they maintain a substantial relationship with the country or region. *Non-resident non-nationals* can sometimes also be catered for, as can be seen in Estonia (Sallam et al., 2022). *Domestic* and *foreign juridical persons*, as entities having a legal status similar to that of a natural person, are also covered in this dimension (OECD, 2023), as well as the special category of *persons without proof of identity* (Madon & Schoemaker, 2021).

Roles of private sector actors: while institutional actors are necessarily involved in the orchestration and supervision of the infrastructure and in the certification of digital identity data, the private sector can be authorized to take part in the provision and use of digital identity services in different ways. *No role* means that the digital identity system is seen as a purely public service for government to government, citizen to government and government to citizen use cases, and is fully delivered by the public sector with no involvement from the private sector. *Authoritative source* provides a trusted source of data for use within the digital identity infrastructure (e.g., Banks in Sweden). *Registrar* is the role tasked with collecting and verifying identity data (e.g., PostIdent in Germany, some Aadhar enrolment agencies in India). *Data managers* (also sometimes called data controllers) manage the identity lifecycle, from creation to revocation (e.g., BankID in Sweden). *Credential providers* can generate and manage credentials and attestations of attributes (e.g., Buypass in Norway). *Trust and orchestration services providers* (or intermediaries) provide services, such as authentication, federation, certificate signing, identity access management and wallet provision (e.g., Aggregators in Italy, Orchestrators in the UK). *Relying* *parties* consume digital identity-related services in the course of their service delivery activities. A combination of the authoritative source, registrar, data manager and credential provider roles is often referred to as an "identity provider" role.

4.2. IT management layer

The ecosystem layer is composed of four dimensions: **operation and ownership**, **software licensing**, **use of standards**, **development funding** and **operational funding**.

Operation and ownership: the IT infrastructure can be managed primarily by the *public sector* (e.g., Singpass in Singapore) and/or by the *private sector* (e.g., BankID in Sweden). Their combination as part of public-private partnerships arrangements can take several forms, such as concessions or service agreements (GSMA et al., 2016), and are increasingly used when building new infrastructure (e.g., ClaveÚnica in Chile, Aadhar in India).

Software licensing: this dimension describes the choice to be made with regards to the openness of technical development of the various modules composing the digital identity system, going from *closed-source* solutions (currently most cases) to *open-source* (e.g., MOSIP implementation in Morocco).

Standards usage: each building block of the digital identity infrastructure can either be *compliant*, or *non-compliant*, to standards, a characteristic that can significantly influence the ease of enabling interoperability, and avoiding vendor lock-in (Medaglia et al., 2022). The European Telecommunications Standards Institute, the National Institute of Standards and Technology and the World Wide Web Consortium are prime examples of standardization bodies which publish standards for digital identity (ETSI, 2021; Grassi et al., 2017; Sporny et al., 2019; W3C, 2022).

Development funding: describes the infrastructure's funding model for the pre-operational phase. The characteristics are *public funding* (including loans from e.g., international development agencies), *grants* (e.g., from donor organizations), and *private funding*. In developing countries, a mix of these options is often used to reduce the upfront investment required from public bodies (Gelb & Diofasi, 2018).

Operational financing: relates to the financing mode characteristics of the operational phase. It targets financial sustainability of operations, including providing a return on investment to private partners who invested in the building of the capacity, when applicable. The characteristics are *public budget*, *charge for identity providers*, *charge for relying parties*, and *charge for subjects*. Very often, a mix of these characteristics come into play, including for example charges to subjects for specific cases (e.g., emergency delivery of a credential). The charge can be measured according to different metrics, such as volume of transactions.

4.3. Data management layer

The data layer is composed of three dimensions: **exchange model**, **linkability** and **trusted data storage**. Design decisions related to this layer directly impact data protection and privacy, and as such are often the subject of much scrutiny both from data protection authorities and citizens (Beduschi, 2021).

Exchange model: identity data, in the form of attributes or bundled in credentials, can be transmitted through different actors. *Identity provider to relying party*: the relying party retrieves identity information directly from the identity provider or the authoritative source (e.g., healthcare providers requesting data to social security entities). *Data subject to relying party*, also sometimes called "self-sovereign identity" (Pöhn et al., 2021): the data subject holds a credential which is directly shared with the verifier (relying party), without the involvement of an identity provider in the data exchange (e.g., the European Digital Identity Framework). *Federation through one actor*: a singular gateway allows for the exchange of data and oftentimes as an authentication provider (e.g., Aadhar in India). Since all identity transactions go through this one actor, this model presents non-benign risks of surveillance that need to be addressed. *Federation through multiple actors*: several actors can act as federation service providers (e.g., FranceConnect in France). This model gives more choice to users and limits the consolidation of data and power within a single entity.

Linkability: linking of identity data, or identity data matching, can take two main governance configurations. Identity data matching can either be *mediated* by a third-party (e.g., the sourcePin Register Authority in Austria), or *non-mediated* (e.g., through a unique identifier, technological means, or simply comparing datasets for common attributes). A framework that establishes the conditions in which data matching is allowed to take place can help avoid cases of illegitimate data matching and inferences (Wachter & Mittelstadt, 2018).

Trusted data storage: data can be stored in different configurations. *Cross-sectoral repositories* merge identity data that do not belong to the same area (e.g., health, taxation). This configuration is often decried as damaging for data subjects' privacy. *Sectoral repositories* hold identity data for one specific sector. Finally, *user wallets* allow data subjects to hold a trusted version of their identity data. In most cases involving user wallets, a copy of the data also remains in a repository to mitigate issues linked to credential loss.

5. Discussion and Conclusion

Digital identity infrastructures have seen a rise in interest from governments wanting to enable participation of their citizens in a digital society and economy. However, recent experiences show that misaligned organizational and institutional arrangements can cause project failures even in rich, developed countries, leading to public distrust, and wasted resources. To overcome this challenge and limit the risks of project failure, strategic governance choices of digital identity infrastructure design must be well identified, understood, planned, and communicated. A clear terminology and systematic guidance can support this objective (Janssen & Helbig, 2018).

In response, we developed a taxonomy of strategic governance choices for digital identity infrastructures following the development process proposed by Nickerson et al. (2013). During this process, we conducted four iterations, leveraging existing knowledge disseminated in scientific and practitioner literature, interviewed 12 specialists, and analyzed 13 existing instantiations of digital identity infrastructures. This resulted in a final taxonomy consisting of three layers, 13 dimensions and 46 characteristics of governance decision domains in digital identity infrastructure, providing an answer to the research question of this paper. Several implications are drawn from our results, applicable for both theory and practice.

Our work contributes to theory through a richer understanding of the under-researched field of governance of digital identity infrastructure. Our taxonomy expands the existing body of knowledge through a consolidation of practitioners and academic insights and establish a consensus-based terminology to support a common understanding on this topic (Rana et al., 2011). This contribution is of value to e-government research on digital infrastructure (Janowski, 2015) and can support other research directions within the wider information systems domain at large (Belanger & Carter, 2012). In brief, the contributed taxonomy can be used to distinguish and depict critical governance aspects of digital identity infrastructures in a systematic and comprehensive way, and serve as contextualization basis for theory-building (Bapna et al., 2004).

We contribute to practice on three levels. First, the list of governance characteristics of digital identity infrastructure, along with relevant design choices, can help practitioners during the design and implementation of such infrastructure. Second, given the concise and explanatory character of the provided taxonomy, we provide policymakers with a tool for contextualization to better assess the design choices that they are faced with (Janowski, 2015), thus answering the call for better research and training resources in the area of digital identity (Wimmer et al., 2020). Third, citizens who are impacted by the deployment and use of digital identity infrastructure are provided with a tool to concisely apprehend the impactful characteristics of governance thereof, consequently helping them make better informed decisions and enable them to steer their design through participative action. It also supports approach uniformity when it comes to successful digital identity infrastructure evolution.

Some limitations of this research must be acknowledged. First, the field of digital identity infrastructure is still relatively nascent and, coupled with the accelerating pace of technological innovation in the realm of identity management, it is likely that this taxonomy will have to be extended in the medium-term. Second, the high level of complexity of the topic should lead us to remain humble about the universal character of the taxonomy, as its focus might have been steered in part by the current challenges facing the digital identity community. Indeed, some of the strategic governance choices facing institutional actors today might evolve, and new governance choices might soon need to be considered in a different light. Finally, while our fourth iteration consisted in an analysis of a representative sample of instantiations of digital identity infrastructure, a systematic evaluation of further existing instantiations could potentially reveal rare characteristics that would deserve to be added.

These limitations lead us to call for further research. To better assist practitioners with actionable knowledge that can be applied within their specific context, case-study based evaluation of the impact resulting from these governance decisions could yield significant insights. While we focused on the governance aspects of digital identity infrastructure, there would also be value in delving into the technical elements that compose the infrastructure and the interplay between these two domains. Finally, there is an opportunity to dig deeper into each of the dimensions of the taxonomy, bringing in a more focused and granular view beyond the strategic design choices.

When well designed and implemented, digital identity infrastructures have the potential to promote economic development and socioeconomic inclusion in the digitalized world (Addo & Senyo, 2021; Wang & Filippi, 2020). Building on the outcome of our research, future research may contribute to the successful actualization of these benefits.

Acknowledgements

The authors would like to thank Tom Barbereau, Linda Weigl, Emanuela Podda and Reilly Smethurst for their review and contributions to the references list.

This research was supported in part by Luxembourg's Ministry for Digitalisation, PayPal and the Luxembourg National Research Fund (FNR), Luxembourg (P17/IS/13342933/ PayPalFNR/Chair in DFS/Gilbert Fridgen) and the FNR in the FiReSpARX (grant reference 14783405) project. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for Development : Digital Identification and its Link to Socioeconomic Inclusion. Government Information Quarterly.

Bailey, K. D. (1994). Typologies and taxonomies : An introduction to classification techniques. Sage.

Bapna, Goes, Gupta, & Jin. (2004). User Heterogeneity and Its Impact on Electronic Auction Market Design : An Empirical Exploration. *MIS Quarterly*, *28*(1), 21.

Beduschi, A. (2019). Digital identity : Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2),

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies : Data privacy and human rights considerations. *Data & Policy*, *3*.

Belanger, F., & Carter, L. (2012). Digitizing Government Interactions with Constituents : An Historical Review of E-Government Research in Information Systems. *Journal of the Association for Information Systems*, *13*(5), 363-394.

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790.

Bijker, W. E., Hughes, T. P., & Pinch, T. (Éds.). (1987). The Social construction of technological systems : New directions in the sociology and history of technology. MIT Press.

Boysen, A. (2019). *The Need for a National Digital Identity Infrastructure* (Governing Cyberspace during a Crisis in Trust, p. 36-40). Centre for International Governance Innovation.

CAG of India. (2021). Report of the Comptroller and Auditor General of India on the Functioning of Unique Identification Authority of India.

Davies, G. (2006). Is Mutual Recognition an Alternative to Harmonization? Lessons on Trade and Tolerance of Diversity from the EU. In L. Bartels & F. Ortino (Éds.), *Regional Trade Agreements and the WTO Legal System* (p. 0). Oxford University Press.

Dawes, S. S. (2009). Governance in the digital age : A research and action framework for an uncertain future. *Government Information Quarterly*, *26*(2), 257-264.

DPGA, & GiZ. (2022, mai). GovStack Definitions : Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf

ETSI. (2021). *TS 119 461*.

Gelb, A., & Diofasi, A. (2018). Identification Revolution : Can Digital ID be Harnessed for Development?

Giannopoulou, A. (2023). Digital Identity Infrastructures : A Critical Approach of Self-Sovereign Identity. *Digital Society*.

Gil-Garcia, J. R. (2012). Enacting Electronic Government Success : An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions (Vol. 31).

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020). Towards a comprehensive understanding of digital government success : Integrating implementation and adoption factors. *Government Information Quarterly*, *37*(4), 101518.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines : Revision 3* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology.

GSMA, World Bank Group, & Secure Identity Alliance. (2016). Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation.

Hanseth, O., & Lyytinen, K. (2010). Design Theory for Dynamic Complexity in Information Infrastructures : The Case of Building Internet. *Journal of Information Technology*.

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2022). Probably Something : A Multi-Layer Taxonomy of Non-Fungible Tokens.

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. *MIS Quarterly*, *37*(3), 907-931.

ITU. (2018). Digital Identity Roadmap Guide. ITU.

Janowski, T. (2015). Digital government evolution : From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221-236.

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle : Policy-makers be prepared! *Government Information Quarterly*, *35*(4, Supplement), S99-S105.

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management*, *5*.

Madon, S., & Schoemaker, E. (2021). Digital identity as a platform for improving refugee management. *Information Systems Journal*, *31*.

Manny, L., Angst, M., Rieckermann, J., & Fischer, M. (2022). Socio-technical networks of infrastructure management : Network concepts and motifs for studying digitalization, decentralization, and integrated management. *Journal of Environmental Management*, *318*, 115596.

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, *31*(6), 903-928.

Masiero, S., & Bailur, S. (2021). Digital identity for development : The quest for justice and a research agenda. *Information Technology for Development*, *27*(1), 1-12.

McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* (NIST SP 800-122; 0 éd., p. NIST SP 800-122). National Institute of Standards and Technology.

McKinsey. (2019). Digital identification : A key to inclusive growth.

Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of power inscription into governance : Lessons from two national digital identity systems. *Information Systems Journal*, *32*(2), 242-277.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation : Results from expert interviews. *Government Information Quarterly*, *36*(4).

National Audit Office. (2019). *Investigation into Verify*.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*, 336-359.

Nyst, C., Pannifer, S., Whitley, E. A., & Makin, P. (2016, juin 8). *Digital identity : Issue analysis*. Consult Hyperion.

OECD. (2023). Recommendation of the Council on the Governance of Digital Identity.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames : Making sense of information technology in organizations. *ACM Transactions on Information Systems*.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1).

PwC. (2021). PwC-Studie : Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche.

Rana, N. P., Williams, M. D., Dwivedi, Y. K., & Williams, J. (2011). Reflecting on E-Government Research : Toward a Taxonomy of Theories and Theoretical Constructs. *International Journal of Electronic Government Research (IJEGR)*, *7*(4), 64-88.

Sallam, M., Lips, S., & Draheim, D. (2022). Success and Success Factors of the Estonian E-Residency from the State and Entrepreneur Perspective (p. 291-304).

Saunders, C., Benlian, A., Henfridsson, O., & Wiener, M. (2020, novembre 23). *IS Control & Governance*. MIS Quarterly.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*, 1-16.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*, 603-613.

Sporny, M., Longely, D., & Chadwick, D. (2019). *Verifiable Credentials Data Model 1.0*. W3C Recommendation.

Temoshok, D., Richer, J., Choong, Y.-Y., Fenton, J., Lefkovitz, N., & Regenscheid, A. (2022). *Digital Identity Guidelines : Federation and Assertions* (NIST Special Publication (SP) 800-63C-4 (Draft)). National Institute of Standards and Technology.

UIDAI. (2023). *Finance & Accounts*. Unique Identification Authority of India | Government of India.

UN Legal Identity Expert Group. (2019). United Nations Strategy for Legal Identity for All.

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, *22*(5), 896-914.

W3C. (2022). Decentralized Identifiers (DIDs) v1.0.

Wachter, S., & Mittelstadt, B. (2018). *A Right to Reasonable Inferences : Re-Thinking Data Protection Law in the Age of Big Data and AI* (SSRN Scholarly Paper 3248829).

Walke, F., Winkler, T., & Le, M. (2023). Success of Digital Identity Infrastructure : A Grounded Model of eID Evolution Success.

Wang, F., & Filippi, P. (2020). Self-Sovereign Identity in a Globalized World : Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, 28.

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU's Digital Identity Policy : Tracing Policy Punctuations. *15th International Conference on Theory and Practice of Electronic Governance*, 74-81.

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of Self-Sovereign Identity : An Extended Model of Interpretive Flexibility. *Proceedings of the Hawaii International Conference on System Sciences 2022*.

Whitley, E. A., & Schoemaker, E. (2022). On the sociopolitical configurations of digital identity principles. *Data & Policy*, *4*, e38. https://doi.org/10.1017/dap.2022.30

Wimmer, M. A., Pereira, G. V., Ronzhyn, A., & Spitzer, V. (2020). Transforming government by leveraging disruptive technologies : Identification of research and training needs. *eJournal of eDemocracy and Open Government*.

World Bank. (2014). Digital Identity Toolkit.

World Bank. (2022a). Federated Ecosystems for Digital ID : Current Approaches and Lessons. World Bank.

World Bank. (2019a). ID4D Practitioner's Guide.pdf.

World Bank. (2019b). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. World Bank.

World Bank. (2022b). Identification for Development (ID4D) and Digitalizing G2P Payments (G2Px) 2022 Annual Report

Challenges in designing digital identity infrastructure for development: A consensus-based taxonomy of strategic institutional and governance choices

Alexandre Amard[a]* and Gilbert Fridgen[a]

*Alexandre Amard, alexandre.amard@uni.lu, [a]Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 29 Av. John F. Kennedy, L-1855 Luxembourg, Luxembourg

Challenges in designing digital identity infrastructure for development: A consensus-based taxonomy of strategic institutional and governance choices

Governments in low- and middle-income countries (LMICs) increasingly deploy digital identity infrastructure. These initiatives are considered a fundamental building block for their citizens to reap the benefits of digitalization and take part in the digital society and economy. But this outcome is not guaranteed: it considerably hinges upon a range of strategic governance decision domains that institutional actors must act on when designing digital identity infrastructures. We analyzed academic and grey literature, archival records of 20 infrastructure instantiations, and conducted 17 expert interviews of practitioners and researchers active in both LMICs and high-income countries (HICs) to propose a consensus-based taxonomy of strategic institutional and governance design choices for digital identity infrastructures. Additionally, we provide an example of possible contextual usage of the taxonomy, uncovering implications for researchers and practitioners active in LMICs and contributing to the digital development literature by setting a foundation for further research and theory-building on digital identity infrastructure.

Keywords: digital identity, digital infrastructure, digital government, information technology for development, governance

1. Introduction

In 2021, an estimated 850m people around the world were lacking means of identification (World Bank, 2021a), challenging the United Nations' Sustainable Development Goal 16.9, *legal identity for all, including birth registration, by 2030* (UN LIEG, 2019). The vast majority of these people (98%) were in low- or middle-income countries (LMICs). Digital identity infrastructure is increasingly considered as a means to tackle this challenge, support sustainable development, and effectively enable society-wide functions and services provided by the government or private sector in developing countries (Henfridsson & Bygstad, 2013; DPGA & GiZ, 2022; Gelb & Metz, 2018). The benefits commonly associated with digital identity infrastructure are multiple, and particularly transformative in LMICs. Both academics and practitioners have highlighted its capacity to support socio-economic development, enable individual agency and improve inclusion.

In light of these asserted benefits, the development of reliable digital identity infrastructure has become a high priority for governments in LMICs to enable their citizens to take full advantage of the opportunities that digitalization represents (Gelb & Diofasi, 2018), and a number of countries around the world have built their own digital identity capabilities, including India, Nigeria, Ethiopia, Peru and the Philippines. Many more commit substantial resources to build or improve their own digital identity infrastructures (World Bank, 2022b). These foundational, interoperable shared digital systems that promote access to digital services for all, are often designated *digital public infrastructure (DPI)* (G20, 2023; UNDP, 2023). Multilateral organizations are launching initiatives to support countries develop and implement these constructs, in a bid to simultaneously accelerate progress towards the Sustainable Development Goals and support the digital transformation of their government (ITU, 2023). These ambitions crystallize into initiatives such as 50-in-5, that target to support countries 'design, launch and scale components of their digital public infrastructure', with support by multilateral banks such as the Inter-American Development Bank and social welfare organizations such as UNICEF (50-in-5, 2023). Due to the fundamental role it plays in delivering digital services across government and society, digital identity infrastructure is considered as one of the three 'core' digital public infrastructures, together with payment and data exchange (G20, 2023; UNDP, 2023).

But despite the level of attention and funding it attracts, examples of successful digital identity infrastructure deployments are relatively few, including in high-income countries (Walke et al., 2023). Many recent initiatives have exhibited varying signs of failure, ranging from low adoption to outright discontinuation, or even citizen rejection prior to implementation. A 2021 PwC survey revealed that Germany's electronic identification scheme had a very low uptake, with only 7% of citizens having used their electronic identity document in 11 years following its introduction (PwC, 2021). In the UK, the GOV.UK Verify infrastructure, that was expected to be taken over by the private sector by 2020, was publicly qualified as a failure (National Audit Office, 2019) and fully discontinued in 2023, a few months after the UK's taxation authority withdrew from the scheme. The total cost for the infrastructure was estimated to be £220m. In Switzerland, the digital identity infrastructure did not even get a chance to start: in March 2021, a referendum saw the adoption of the Electronic Identification Services Act overwhelmingly rejected (Swiss Federal Counsel, 2021). This failure was largely attributed to the role that the private sector would have taken in provisioning digital identities. Again in 2021, the Comptroller and Auditor General of India heavily criticized the Unique Identification Authority of India's (UIDAI) national digital identity infrastructure Aadhaar, not least because of the poorly established relationship between government and private sector partners (CAG of India, 2021). To build and manage its identity infrastructure, the UIDAI spent Rs 15764.48 Crore (~$1.8bn) from its inception in 2009 until February 2023 (UIDAI, 2023d). If failure in HICs is of course unfortunate, the cost of failure in LMICs can often affect entire livelihoods, especially for women, minorities and populations at risk who disproportionately depend on the actualization of the benefits promised by digital identity infrastructures. Failure costs can concretize in different ways: financial costs, opportunity costs, political costs, future costs and, probably even more regrettably, beneficiary costs (Heeks, 2003). In many cases including the ones just mentioned, failures were widely attributed to what Heeks identified as *design-reality gaps,* i.e., mismatches between design and actuality of users. These mismatches appeared as a result of strategic design choices of *governance*; conceptualized in this paper as the macro-level choices happening at the intersection between relational governance, corporate governance and infrastructure governance (Saunders et al., 2020).

The importance of governance arrangements has long been established, and their mechanisms studied extensively. Public-private links, service diversity, user awareness and acceptance, regulation and organizational structures are governance-related factors that can influence the success of digital identity infrastructure (Walke et al., 2023). Additionally, both organizational and institutional arrangements impact the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), reinforcing their central role in realizing the infrastructure’s value. This challenge is compounded by the fact that institutional actors are confronted with a myriad of governance design options for digital identity infrastructure. These choices will impact the infrastructure, the services that rely on it and its users for years, if not decades. In other words, borrowed to the OECD, (2023):

> To ensure the long-term sustainability of digital identity, governments need to establish robust governance foundations and treat digital identity as critical digital public infrastructure.

A detailed look at instantiations around the world reveals wildly different implementations and substantial design complexity. For example, in Scandinavian countries, banks play a crucial role in providing digital identity services to citizens who use their ‘BankID’ on a daily basis for various identification purposes (Husz, 2018). On the other hand, some countries such as Spain have built their digital identity capabilities around public sector needs (Rocha, 2020), and the private sector is primarily acting as a subcontractor. The Indian Aadhaar system is led by the public sector, with extensive participation of the private sector, including for the enrolment of citizens (UIDAI, 2023c). Aadhaar is also widely centralized with identity data stored in a governmental database linked together by the 12-number Aadhaar number and biometric characteristics (Pali et al., 2020). On the other side of the spectrum, Bhutan recently adopted a bill establishing a digital wallet enabling its citizens to assert control on the disclosure of their identity data during identification and authentication transactions (Parliament of Bhutan, 2023). These are just a few of the existing governance configurations in an area where disruptive technologies are increasingly deployed. Then, how can institutional actors have confidence that they evaluated the most important governance design options? What are the governance choices available to them that will have substantial impact on the design and ultimate success of the costly infrastructure? How will these choices support, or hinder, the actualization of the infrastructure’s benefits? Despite their criticality, so far, no consolidated answer to these complex questions has been offered. While some of the topics at hand are individually addressed in literature, to our knowledge, there is no systematic guidance and terminology on the strategic institutional and governance choices for digital identity infrastructure. In response, we formulate the following research questions:

> RQ1: What are the design choices for governing the development and operations of digital identity infrastructure?
> RQ2: How can they impact the actualization of digital identity benefits in an LMIC context?

Answering these questions requires first and foremost to understand, classify, and systematically structure common characteristics of the strategic governance choices available when designing digital identity infrastructure. We thus selected a classification method that is highly valued in information systems research when it comes to structuring and organizing the body of knowledge in complex and novel areas of research (Glass & Vessey, 1995), taxonomy development. On the one hand, taxonomies help both researchers and practitioners understand and analyze complex domains (Nickerson et al., 2013), which is in line with our recognition that the outcome of this research should serve both these stakeholder communities. On the other hand, they can also serve as relevant input for the development of theories and for hypothesis generation and testing (Doty & Glick, 1994; Iivari, 2007), which helps us on the path to answer our second research question.

In particular, we selected the taxonomy development process of Nickerson et al. (2013), whose rigor is acknowledged by the most reputable scientific outlets (Kundisch et al., 2022). Our development process involved seven iterations, which included a literature review, analysis of archival records, elite interviews with practitioners and researchers active in the field of digital identity infrastructure in both LMICs and HICs, and an analysis of governance models of existing or ongoing infrastructure deployments. While our focus in this paper is on LMICs, we included both LMICs and HICs in our analysis, as the experience of developed countries can be useful for developing countries (Janssen & Helbig, 2018) and because countries in different categories can still exhibit common contextual elements that would make decisions appropriate in each case. Further, we instantiated this taxonomy in order to reveal its capacity to generate insights related to our second research question, and guiding researchers and practitioners towards its usage in context.

Our findings include that both academic and practitioner communities were widely in agreement regarding what constitutes strategic governance design choices for digital identity infrastructure. This challenged our initial concern about their potential subjectivity. We further found that, when instantiated, our taxonomy can indeed act as an insight-generating analytical lens for both longitudinal case studies and thematic analysis. We put these qualities in the spotlight through an instantiation that reveals some of the key dynamics through which governance decisions impact the actualization of benefits in a LMIC context. Together, these findings contribute to a better understanding of governance choices for digital identity infrastructure, and the impact thereof, in an accessible format.

This paper is structured as follows. In section 2, we present the theoretical background regarding digital identity, digital identity infrastructure, and their expected benefits and risks in LMICs. We then discuss the implementation of our research method in section 3, which we used to develop a multi-layer taxonomy presented as our research findings in section 4. Section 5 is then dedicated to an 'in-situ' instantiation of the taxonomy and to its accompanying discussion, showcasing its interpretive and hypothesis-building qualities across two examples in context. In section 6, we present a reflection of our findings, acknowledging their implications for research and practice as well as their limitations, and proposing avenues for future research before concluding in section 7.

2. Theoretical Background

In this section, we provide an overview of the key theoretical themes pertaining to the topic of digital identity infrastructures and their role in development, as well as the main research directions through which they have been addressed in the scientific and grey literature.

2.1. Digital identity

Our research is concerned with the identity of physical persons due to the critical development challenges it presents, but we should note that digital identity is also increasingly applied to legal entities (Leung et al., 2022) as well as objects in an IoT context (Bartolomeu et al., 2019). In this article, we conceptualize *digital identity* as the set of digitalized identity attributes and credentials that describe qualities, characteristics, or assertions of a *person* (Temoshok et al., 2022). This digital identity can be used for the identification and authentication of a person via digital channels, for instance, to provide governmental and private sector services (Nyst et al., 2016). In turn, digital credentials are the means through which a data subject can assert these qualities, characteristics and assertions (Sedlmeir et al., 2021). Digital credentials can take several forms, ranging from electronic identity documents to smartphone-stored digital documents, and are sometimes enhanced with other authentication factors such as biometrics or passwords to allow for a higher level of authentication assurance (World Bank, 2019a). A digital credential can also simply be a reference to a digital record in a database, or directly contain identity attributes. Cryptographic methods are employed to ensure the integrity and authenticity of credentials (Sedlmeir et al., 2021), while safeguards and controls are used to support data protection and prevent data leakage and identity theft (McCallister et al., 2010).

Digital identity emanates from entities in charge of collecting and verifying identity data about a subject and translating it into the digital realm. As digital identity is not a monolithic construct, identity data and credentials making up a digital identity can be collected, stored, certified, and issued by different stakeholders (Grassi et al., 2017). These authoritative entities hold data that is accepted as accurate and trustworthy within a particular sector of application (e.g., taxation, criminal records, and health). In many countries, linkability of identity data (e.g., through unique identifiers or mediating entities), which allows for the re-identification of a data subject in different circumstances, is strictly regulated for privacy and data protection purposes (Beduschi, 2019). The capacity to materialize the benefits of digital identity, including the capacity to collect, store and verify identity attributes, enroll and authenticate users, and manage credentials and authorizations, requires the establishment of a digital identity infrastructure (Nyst et al., 2016).

2.2. Digital identity infrastructure

Digital identity infrastructures can be defined as systems that construct, control, and commodify (facets of) digital identities and can be formed by both public and private sector actors (Giannopoulou, 2023). They are an operationalization of digital infrastructure, i.e., digital, socio-technical systems that underlie or support the public interest, as well as universal or quasi-universal services (Plantin et al., 2018). Despite many having a national dimension, some digital identity infrastructures target transnational interoperability (e.g., the West Africa Unique Identification for Regional Integration program, or the European Union's electronic Identification, Authentication and Trust Services regulation (eIDAS)). Others, in turn, operate at the sub-national level (e.g., the Ontario and Alberta provinces). Digital identity infrastructures conceptualize the reality of interconnected system collectives, which evolve at the intersection between socio-technical elements, networks of actors and relationships between organized practices (Henfridsson & Bygstad, 2013), and are thus to be considered within the complex socio-technical systems that structure them (van Dijck & Jacobs, 2020; Weigl, Barbereau, et al., 2022). Organizational and institutional arrangements significantly influence the selection, design and implementation of information technologies in government (Gil-Garcia, 2012; Koppenjan & Groenewegen, 2005; World Bank, 2014), thus playing an important role in the design of digital infrastructure. It follows that considering actors, roles, people and processes is a necessary condition for the development and implementation of useful and sustainable infrastructures (Dawes, 2009; Manny et al., 2022). Digital identity infrastructure design and success are therefore inextricably interlocked with the strategic governance choices that impact them (Gil-Garcia & Flores-Zúñiga, 2020; Medaglia et al., 2022), and their identification and characterization should be a priority.

2.3. Expected benefits and risks in LMICs

Digital identity infrastructures are credited with enabling various potential benefits, including 'facilitat[ion] and simplif[ication of] access to a wide range of services and thereby contribut[ion] to social and economic value' (OECD, 2023), better 'inclusion, social protection, healthcare and education, gender equality, child protection', 'delivery of public services and programs', and the 'reduction of fraud' (World Bank, 2019b). The primary driver for these benefits is the capacity of digital identity systems to provide a form of legal identity, a prerequisite to fully participate in society, assert rights and be considered for entitlements. This can be particularly impactful in LMICs, where many people depend on social assistance (Hanna & Olken, 2018) and have difficulties accessing essential services (Cicchiello et al., 2021). There, digital identity infrastructure can be used to support welfare delivery through e.g., cash transfer programs, and support citizens social and economic inclusion through access of e.g., financial services (Sharma & Díaz Andrade, 2023). Gelb & Diofasi (2018) list the far-reaching implications of identification on sustainable development goals (SDGs) and their impact on populations. These include better access to finance (an estimated 30% of people in developing economies were unbanked in 2021 (World Bank, 2021b), access to basic services, labor market opportunities, social protection and managing public payrolls, and address a wide range of SDGs and their related goals. As a consequence, McKinsey (2019) expects that countries successfully implementing digital identity infrastructure could 'unlock value equivalent to 3 to 13 percent of GDP by 2030', with most of the value accruing to individuals in emerging economies. But economic development is not the only development outcome that LMICs can expect from digital identification. Social inclusion can be improved through better citizen participation in the economy and society which in turn can generate 'cross-generational improvements by increasing access to education and enabling communities to collaborate' (Blakstad & Allen, 2018 p.130; Wang & Filippi, 2020). Digital identity can also be used as a foundation for increased voting participation and to improve trust in the democratic process. This improved civic and political participation can in turn strengthen democratic institutions (Bhatt et al., 2021; Dahan & Hanmer, 2015). On a theoretical level, Addo & Senyo (2021) contend that these dynamics can be explained by digital identification's mediation role in fulfilling entitlements and expanding citizens and residents capabilities and functioning. Digital identity infrastructure can also act as a vector of efficiency by streamlining identification in countries where identity databases have been built for functional purposes (e.g., voters' registries, social services).

On the other hand, a more critical view has also been adopted by scholars and practitioners alike. Implementation of digital identity infrastructure have been denounced for generating adverse impacts, such as ‘exclusion from access’, ‘distortion of monitoring’, ‘redirection of policy’ (Masiero & Arvidsson, 2021) and ‘privacy and security violations’ among others (Beduschi, 2019; World Bank, 2019a). To contrast with an optimistic discourse focusing on the potential benefits of the infrastructure, some scholars have argued that in some forms, they go so far as to ‘undermine the right to life’ (Khera, 2017). These conflicting views have been well commentated, (see e.g., Weitzberg et al., (2021)), and our research fully acknowledges the accompanying debate, although it neither intends to take a position on it nor settle it. Rather, it accepts the premise that digital identity infrastructures are widely being considered and deployed across the world, and that research supporting a better understanding of these constructs can only help structure, and maybe instruct, some aspects of this debate.

3. Research method

In this section, we present our research method, the rationale for selecting it, and the way we operationalized it. We detail our data collection approach, which consisted of reviewing academic and grey literature, conducting elite interviews with researchers and practitioners, and analyzing existing digital identity infrastructures. Further, we detail how, through seven iterations and systematic evaluation of ending conditions, we transformed this qualitative input into a consensus-based taxonomy.

3.1. Methodology selection rationale

Faced with the complexity of the research topic at hand and aiming to support future studies and real-world implementations of digital identity infrastructures, we adopt a systematic qualitative approach with the aim of producing verifiable, reproducible insights. We select the taxonomy development process as methodological approach, due to its capacity to structure and organize the body of knowledge and thus support us answering our first research question: *RQ1 What are the design choices for governing the development and operations of digital identity infrastructure?* Taxonomies can also act as a foundation for hypothesis-making (Glass & Vessey, 1995) and theory-building (Bapna et al., 2004), thus forming a useful foundation to answer our second research question: *RQ2 How can they impact the actualization of digital identity benefits in an LMIC context?* Further, taxonomies can serve as a foundation upon which research and practice can build (Bapna et al., 2004), supporting our objective of addressing scholars, policymakers, and practitioners in the field of e-government and international development. Finally, taxonomies are widely utilized in both information systems research and development studies (see Berger et al., 2020; Diniz et al., 2019; Drasch et al., 2018; Hartwich et al., 2022; Perez et al., 2019) and thus are appropriately familiar for researchers and practitioners to support its wide usage.

This methodology also helps us answer several criticisms faced by information and communications technology for development (ICT4D) researchers. By transparently and systematically applying a rigorous and widely accepted methodology, we address the lack of rigor in methodological approach highlighted by Schelenz & Pawelec (2021). Additionally, building a taxonomy also allows us to answer the call for the elaboration of shared conceptual frameworks, ontologies and vocabulary for researchers and practitioners (ibid.).

In order to develop our taxonomy, we structure our approach following the method outlined by Nickerson et al. (2013). This iterative process, as illustrated in **Figure *1***, consists of seven steps which are considered completed once defined ending conditions are met. We rigorously followed this process to ensure reproducibility of our results.

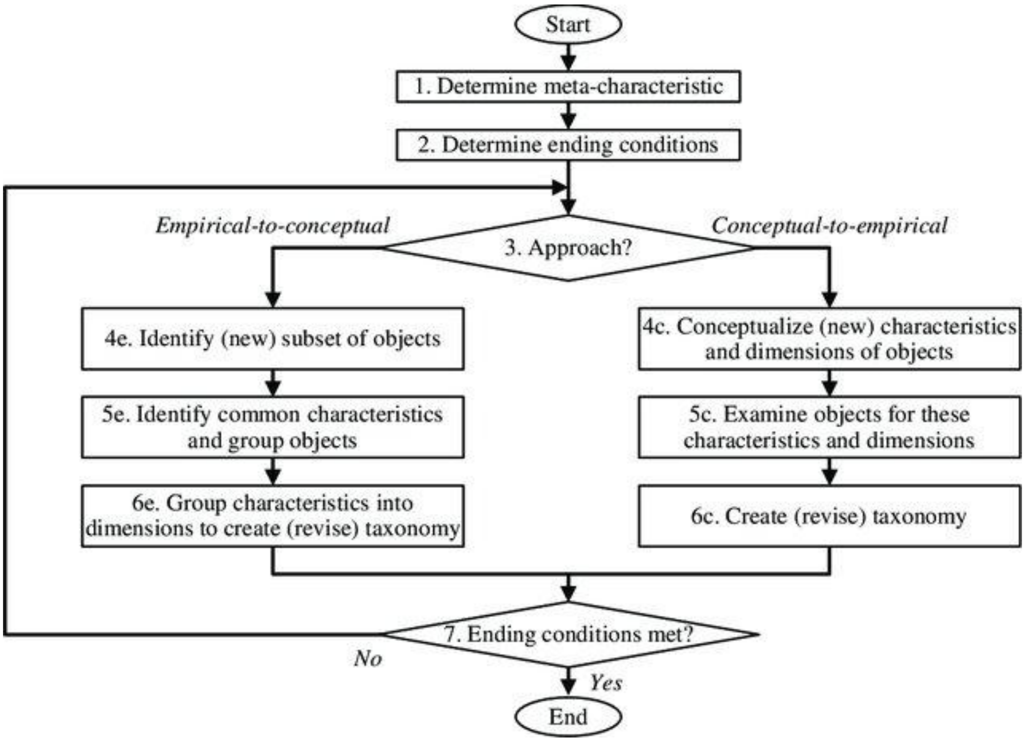

Start
1. Determine meta-characteristic
2. Determine ending conditions
Empirical-to-conceptual
3. Approach?
Conceptual-to-empirical
4e. Identify (new) subset of objects
5e. Identify common characteristics and group objects
6e. Group characteristics into dimensions to create (revise) taxonomy
4c. Conceptualize (new) characteristics and dimensions of objects
5c. Examine objects for these characteristics and dimensions
6c. Create (revise) taxonomy
7. Ending conditions met?
No
Yes
End

Figure 1. Taxonomy development method (Nickerson et al., 2013)

3.2. Taxonomy development process

3.2.1. Determination of the meta-characteristic

Determining the right meta-characteristic is a key steppingstone for the subsequent elaboration of the taxonomy. Indeed, the meta-characteristic influences the scope and boundaries of the taxonomy, including the selection of layers, dimensions, and characteristics that are selected for inclusion into the taxonomy (Nickerson et al., 2013). Its selection needs to allow the research question to be answered. In the case of complex constructs such as digital identity infrastructure, finding the right level of granularity is of paramount importance. It needs to be broad enough to tackle an important research dimension, and precise enough to lead to a substantial and useful contribution. It also needs to be concise in order to avoid becoming difficult to comprehend and to apply (Nickerson et al., 2013). With our research question concerning the institutional and governance aspects that shape digital identity infrastructure for physical persons, our meta-characteristic was appropriately selected as ‘Strategic Institutional and Governance Characteristics of Digital Identity Infrastructure’. This meta-characteristic in turn defines which *dimensions* will be retained for classification and organization. This dimensions act as a categorization level for *characteristics*, i.e., the specific features that help differentiate objects under scrutiny within a particular dimension. For clarity and readability purposes, we elected to additionally group dimensions into *layers*.

3.2.2. Determination of ending conditions

Ending conditions are a critical element of the taxonomy-building process, in that they allow to decide when to stop the iterative process. Objective ending conditions target the formal aspects of taxonomy building and indicate that the taxonomy building process and its iterations can be concluded once they are met (Nickerson et al., 2013). Besides objective ending conditions, subjective ending conditions play an important role as they relate to the usefulness of the taxonomy, which is the primary desired characteristic of the taxonomy.

We set out to validate every objective ending conditions as outlined by Nickerson et al. (2013). These can be broadly classified into 3 categories:

Category	**Objective ending condition according to Nickerson et al. (2013)**
(1) The last iteration should not have induced any needed change in the taxonomy	No new dimensions or characteristics were added in the last iteration
	No dimensions or characteristics were merged or split in the last iteration
	Every dimension is unique and not repeated
	Every characteristic is unique within its dimension

(2) There should be no repetition or duplication between dimensions and characteristics	Each cell (combination of characteristics) is unique and is not repeated
(3) All objects, or a representative sample thereof, have been analyzed, and all characteristics could be identified in at least one object	Every characteristic can be found in at least one digital identity infrastructure
	A representative sample of digital identity infrastructure has been examined

Table 1. Objective ending conditions (based on Nickerson et al. (2013)).

These conditions were tested at the end of each iteration, and we devoted two iterations to specifically analyze a representative sample of objects, i.e., *instantiations of digital identity infrastructure*. An exhaustive analysis of all existing digital identity infrastructures is not feasible, not only because of the important number of instantiations in existence, but also because they evolve rapidly, and limited information is readily available for many of them. We thus selected a sample of 20 instantiations that are widely referred to as archetypes for specific dimensions of digital identity infrastructure governance and thus influenced the governance models of other instantiations. These present particularly interesting and salient characteristics, and their geographical coverage is varied.

As regards subjective ending conditions, we systematically requested an assessment of our taxonomy's usefulness, robustness (i.e., does it enable sufficient differentiation between objects of interest), and explanatory character from our interview partners, who would later use this taxonomy in their work and thus are the best placed to provide feedback. We also used the taxonomy in a digital identity infrastructure design project in an LMIC, during which propositions on the institutional and governance characteristics of the infrastructure were produced, enabling us to evaluate its usefulness in a real-world scenario.

3.3. Iterations

We conducted seven iterations to meet the ending conditions and reach the final version of the taxonomy, where the first four were presented at a conference (Anonymous, 2024). These iterations used various data collection methods, relying on both primary and secondary sources, and took both Conceptual-to-Empirical (C2E) and Empirical-to-Conceptual (E2C) approaches to ensure a multifaceted perspective. The C2E approach is concerned with conceptualization / deduction from theory, while the E2C approach uses empiricism / induction by analyzing existing objects to derive the elements of the taxonomy (Nickerson et al., 2013).

The following table summarizes the iterative process, and the resulting quantitative outcome of each iteration:

ID	Approach	Method	Outcome (L = Layers, D = Dimensions, C = Characteristics)
	Strategic Governance Characteristics of Digital Identity Infrastructure		
1	C2E	Literature review	4L - 9D - 28C
2	E2C	8 elite interviews (practitioners)	4L - 12D - 47C
3	E2C	4 elite interviews (researchers)	4L - 13D - 46C
4	E2C	13 instantiations examination	3L - 13D - 46C
	Strategic Institutional and Governance Characteristics of Digital Identity Infrastructure for Physical Persons		
5	C2E	Literature review and archival records analysis	4L - 13D - 43C
6	E2C	5 elite interviews (practitioners)	4L - 12D - 43C
7	E2C	7 instantiations examination	4L - 12D - 43C

Table 2. Summary of the taxonomy building iterative process

Iteration 1 - C2E: Our first iteration took a conceptual to empirical approach and built on existing academic and practitioner-sourced material dealing with classification of digital identity management systems. We searched the existing body of academic and grey literature dealing with governance of digital identity infrastructure. The search was performed on both academic databases (IEEE Xplore, SAGE Journals, ScienceDirect, SCOPUS and Taylor & Francis), and on the Google search engine, using the search strings ‘digital identity governance’ OR ‘digital identity infrastructure’ OR ‘digital infrastructure governance’. We primarily used this initial phase to identify works of relevance for a second stage of backward and forward searching, i.e., the collection of pieces of work that cite, or are cited by, this initial list of articles. This process allowed us to identify the most relevant work in this area, yielding 65 articles and documents, 32 from academic literature and 33 from grey literature. The work of the National Institute of Science and Technology (Grassi et al., 2017), the International Telecommunication Union (ITU, 2018) and the World Bank (World Bank, 2014, 2022a, 2019a) were particularly useful during this iteration due to their attempt to take a holistic look at digital identity infrastructure, and helped lay down the foundations of the taxonomy. We could additionally identify several dimensions and characteristics that would remain until the final version of the taxonomy. In total, we identified nine dimensions and 28 characteristics. This iteration confirmed that while some useful knowledge supporting the answering of our research question had been synthesized, content was spread out and the vocabulary used varied significantly.

Iteration 2 – E2C: The second iteration took an empirical to conceptual approach and consisted in the interview of eight practitioners. They were selected for their expertise and experience (Mergel et al., 2019) in the design of governance arrangements of digital identity systems: all of them being recognized public figures in the digital identity infrastructure domain (see **Table *5*** in the Appendix for a full overview of interviewees). The interviewees came from both the public and the private sector, and the semi-structured interviews (Schultze & Avital, 2011) lasted between 30 and 90 minutes. Several participants had been involved in the design of multiple digital identity infrastructures in LMIC, which enabled them to adopt a global, synthetic perspective and have empirical experience of causal relationships between institutional governance decisions and their impact. At the beginning of the interviews, we succinctly presented our taxonomy development approach and explained its intended purpose. We then systematically went through the taxonomy, dimension by dimension, characteristic by characteristic, and requested feedback from the interview partner. Our primary purpose was to collect any missing dimensions or characteristics. When our interview partners deviated from the formal taxonomy itself, we did not interrupt and collected their inputs, which became useful for our instantiations. Before ending the interview, we requested an assessment of the taxonomy's usefulness, robustness and explanatory character. This iteration enabled us to both expand the taxonomy and refine it towards meeting our subjective ending conditions. In total, we identified 12 dimensions and 47 characteristics. Towards the end of the iteration, we noticed that we approached theoretical saturation as no new dimensions or characteristics were being identified. All participants agreed that the taxonomy was meeting our subjective ending criteria. On top of their assessment of its usefulness, the robustness and explanatory character were also evaluated through their intuitive understanding of the taxonomy, their capacity to easily distinguish between the characteristics identified, and their unprompted capacity to come up with examples associated with the characteristics.

Iteration 3 – E2C: To ensure rigor, we conducted a third iteration with an empirical to conceptual approach, that consisted in the interview of four researchers with high expertise in the field of digital identity infrastructure and e-government. These semi-structured interviews also lasted between 30 and 90 minutes. Aside from bringing back a previously dismissed dimension and clarifying some of the vocabulary, this iteration did not yield any substantial changes to the taxonomy, thus confirming theoretical saturation. This iteration mainly supported us in improving the comprehensiveness, conciseness and explanatory character of the taxonomy (Nickerson et al., 2013). In total, 13 dimensions and 46 characteristics were retained. Subjective ending conditions were assessed in the same way as in the previous iteration, with the same outcome.

Iteration 4 – E2C: To validate our final ending condition, i.e., the adequate representation of a representative sample of objects, we proceeded with an empirical to conceptual approach, analyzing instantiations of 13 digital identity infrastructures. The instantiations were selected with several criteria in mind: 1. To cover a wide range of geographies and population sizes, 2. To cover a mixture of low-, middle- and high-income countries with different levels of digital maturity, and 3. To account for instantiations widely referred to as 'models' for a particular characteristic. This resulted in the selection of the following countries: Argentina, Australia, Canada, Chile, Estonia, France, Germany, India, Italy, Morocco, Nigeria, Sweden, United Kingdom. This iteration did not yield any further change compared to the previous iteration. The fact that, on the basis of the information available to us at the time of writing, all objects fit within our taxonomy and all characteristics were used, confirmed that we had met all the ending conditions and could conclude the taxonomy development process for this meta-characteristic.

The outcome of iteration 4 was developed to be presented at a conference (Reference anonymized). During this process, it received positive feedback and additional relevant propositions for further improving its usefulness. Following feedback received since acceptance of the paper, it was decided to extend the meta-characteristic of the taxonomy to involve *institutional* aspects as well as governance aspects, and to focus exclusively on physical persons to increase the taxonomy's appropriateness in light of its complexity. It was also used to support the development of an institutional and governance framework for a digital identity infrastructure for a national government in a Western African LMIC, a process during which it was confronted with additional feedback from the field. Following the enthusiasm of both the research and practitioner communities and the acceleration of the importance that the topic has taken since the submission of the conference paper, it was decided to expand the taxonomy taking into account the newest developments in the field.

Iteration 5 – C2E: We thus conducted a fifth iteration with the extended meta-characteristic. It took a conceptual to empirical approach, leveraging practitioner literature on the topic of the institutional settings of digital identity infrastructure and in particular new publications following the crystallization of digital public infrastructure development initiatives. The recent works of the UNDP (UNDP, 2023), the ITU (ITU, 2023) and the OECD recommendation on governance of digital identity (OECD, 2023) were among the key literature incorporated in the analysis. During this iteration, we also seized opportunities to streamline some characteristics and restructure them to simplify the taxonomy. This resulted in the addition of a layer, one dimension with four characteristics, the combination of two dimensions and the rewording of some dimensions. In total, the taxonomy consisted in 4 layers, 13 dimensions and 43 characteristics.

Iteration 6 – E2C: This iteration took an empirical to conceptual approach in order to evaluate the new additions of iteration 5. It consisted in interviews conducted with 5 experienced professionals, currently or recently involved in the design of institutional and governance frameworks of digital identity infrastructure in various geographies. The interviews followed the same protocol as within iteration 2 and 3. At the end of this iteration, no new dimension was added, which confirmed that our refined taxonomy had once again reached theoretical saturation following the expansion of the meta-characteristic. Additionally, all interviewees commended the taxonomy for its usefulness, and confirmed that they would likely use it as a framework for their future work.

Iteration 7 – E2C: In order to fully validate ending conditions, we conducted a final conceptual to empirical iteration consisting in the re-analysis of the 13 instantiations within the updated taxonomy, and the subsequent analysis of seven further instantiations, including ones in progress: Belgium, Benin, Luxembourg, Guinea, the Philippines, Senegal and the EU Digital Identity Framework. During this iteration, we did not identify any new characteristics. In addition, we found that the streamlined taxonomy made the process of classification more straightforward, making us confident that the usefulness of the taxonomy had been improved through iterations 5 to 7. The successful validation of both objective and subjective ending conditions thus confirmed that we could close the taxonomy development process.

4. Taxonomy of digital identity infrastructures

In this section, we present the outcome of the seven iterations of our taxonomy development process. The final taxonomy consists of 4 layers, 12 dimensions, and 43 characteristics. Except for the first dimension (authority governance model), none of the characteristics are mutually exclusive, meaning that a combination thereof is possible.

When building the taxonomy, it rapidly became evident that the complexity of the constructs under investigation made the number of identifiable variants and characteristics of interest extremely large. We thus had to strive to avoid the pitfall of descriptive work and instead focus on identifying explanatory qualities in our retained dimensions and characteristics (Bailey, 1994). In keeping with this philosophy, we maintained our focus on the impactful, or *strategic*, institutional and governance choices presenting viable alternatives, thus refraining from including dimensions and characteristics that could only serve to describe objects in our domain of interest but do not present a significant impact on its value proposition. Similarly, we exclusively focused on true governance *design options*, as opposed to *best practices*, as they were outside of our meta-characteristic and therefore the scope of this specific research project. We thus did not attempt to build an exhaustive list of the commonly agreed preconditions for establishing a digital identity infrastructure, such as a clear regulatory environment, considerations of user involvement, outreach, and procurement hygiene, to name just a few.

In the following section, we illustratively refer to examples and instantiations that were identified during our data collection exercise.

	Layer	Dimension	Characteristics				
Strategic Institutional and Governance Choices for Digital Identity Infrastructure	Institutional Arrangement	**Authority governance model** *(mutually exclusive)*	Inter-ministerial entity	Ministerial entity	Semi-autonomous entity (with stakeholder representation)	Fully autonomous entity (with direct Cabinet- or Executive-level reporting)	
		Additional authority prerogatives	Civil registration	Identity document and certificates issuance	Others (e.g. statistics, digitalization strategy)	Single purpose authority	
	Ecosystem Management	**Subjects**	Nationals (residents)	Nationals (non-residents)	Non-nationals (residents)	Non-nationals (non-residents)	Persons without proof of legal identity
		Geographical scope	Sub-national	National	Transnational		
		Interoperability approach	None	Mutual recognition	Harmonization		
		Interoperability enablers	Standards (technical, organizational, semantic)	Certification or accreditation mechanisms	Open-source / community software		
		Roles of private sector actors	None	Identity consumption	Identity provision	Registrar	Infrastructural provision
	Funding Management	**Development funding**	Public funding	Public-private partnership	Grant		
		Operational financing	Public budget	Charge for relying parties	Charge for data subjects	Other	
	Data Management	**Data presentation model**	Identity provider to relying party	Federation through 1 actor	Federation through multiple actors	Data subject to relying party	
		Identity matching approach	Mediated	Non-mediated			
		Trusted sources	Government-controlled databases	Digital wallets	Distributed ledgers		

Table 3. Final taxonomy of strategic governance choices for digital identity infrastructures.

4.1. Institutional arrangement layer

The institutional arrangement layer is composed of two dimensions: **authority governance model** and **authority affiliation**.

Authority governance model (mutually exclusive): describes how the authority responsible for setting policies and standards, certifying partners and supervising implementation is governed. This can take the following forms. *Inter-ministerial entity*: an arrangement in which the authority is shared as part of an inter-ministerial delegation (e.g., France). *Ministerial entity*: the authority is given to an entity within an existing ministry (e.g., the Ministry of Interior and Transportation in Argentina). *Semi-autonomous entity with stakeholder board representation*: the authority is given autonomy from a ministry, but the governing board has governmental stakeholder representation (e.g., Nigeria). *Fully autonomous entity with Direct Cabinet- or Executive-level reporting*: the authority is autonomous and is only reporting to the highest levels of government (e.g., Ghana). While an autonomous authority is sometimes considered as the 'modern' arrangement (World Bank, 2019a), there is no clear evidence that it results in measurably better outcomes than authorities that have significant ministerial board presence or that are directly affiliated to a ministry. However, authority independence was considered an effective risk-mitigating measure in cases where conflicting interests could influence decision-making with regards to the infrastructure and its usage, and thus the trust that citizens place in them (Okunoye, 2022). Choices made within this dimension do not preclude consultation of other actors and their participation as counsel (including the private sector).

Additional authority prerogatives: while the authority can be a *single purpose authority* that has digital identification and authentication as its sole prerogative (e.g., the France Identité Numérique Interministerial Program), its responsibilities can also include *civil registration* (e.g., the NCRA in Sierra Leone), *identity document and certificates issuance* (e.g., ANIP in Benin), and *other prerogatives* such as statistics (e.g., the PSA in the Philippines), general government digitalization and interoperability (e.g., the Ministry for Digitalization in Luxembourg). With digital identification being highly dependent on the existence and accessibility of high-quality data enabling the unique identification of subjects, risks of exclusion from access are non-negligible for those services that rely on digital identification (Masiero & Arvidsson, 2021). While not a silver bullet, a strong link between civil registration and digital identification efforts was seen as an opportunity to reduce the likelihood of this risk materializing at the individual scale (Gelb & Diofasi, 2018). Capabilities in identity document issuance, personalization and delivery could also be a key asset in ensuring that eligible citizens are able to assert their identity. Indeed, digitally verifiable credentials can increase the level of assurance in the certificate's integrity, authenticity and validity compared to purely physical counterparts, and be helpful to fight against identity theft (Sedlmeir et al., 2021).

4.2. Ecosystem management layer

The ecosystem management layer is composed of four dimensions: **subjects, geographical scope**, **interoperability approach**, **interoperability enablers** and **roles of private sector actors**.

Subjects: different categories of subjects can be included in the digital identity system. *Resident nationals* are often the primary target group, but *non-resident nationals* and *resident non-nationals* are also often considered as they maintain a substantial relationship with the country or region. *Non-resident non-nationals* can sometimes also be catered for, as can be seen in Estonia (Sallam et al., 2022). The special category of *persons without proof of identity* (Madon & Schoemaker, 2021) is also covered within this dimension, which can be integrated into the national digital identity infrastructure or as part of dedicated projects using e.g., UNHCR's Population Registration and Identity Management Eco-System platform (Schoemaker et al., 2021). The choice of which data subjects are part of the digital identification capabilities of the infrastructure raises important questions of data justice, which we address in the discussion section.

Geographical scope: describes how the system relates to the sovereign state. It can be *sub-national* (e.g., a region, state or territory), which is typical in federal states such as Canada or Australia. These might have an additional interoperability layer at the national level. *National* systems are common in non-federal states, such as Peru or Morocco. The *transnational* characteristic highlights that some systems are meant to be usable across borders, as is the case for eIDAS in Europe or WURI in Africa. In the absence of clear accountability and responsibilities at each level, coexistence of these characteristics was identified as a source of undesirable effects. For citizens, confusion can arise as to which entity is responsible for which process. For administrations, it might entail interoperability issues. Canada, a country which falls in both the *sub-national* and *national* categories, addresses this issue by focusing on building a consensus-built framework, including common definitions and open standards, rather than forcing a technological approach (Abraham, 2020). In the European Union, identity is a clear mandate of Member States (Weigl, Amard, et al., 2022). However, legislative and implementing acts mandate precise specifications as to the governance, process and technology to be implemented to attain transnational interoperability, including reporting obligations, the necessity to deliver a digital wallet, to notify at least one electronic identification scheme (Schwalm & Alamillo-Domingo, 2022).

Interoperability approach: defines if and how interoperability with other systems is provided. It can be the case that *no interoperability* is foreseen. While some digital identity systems do not foresee interoperability with other systems, several digital identity systems strive to be interoperable with one another (e.g., eIDAS-notified identity schemes). One approach to achieve such interoperability is *mutual recognition*, meaning that participants to the interoperability implementation effort accept to recognize digital identities issued by another state despite discrepancies between the rules and procedures of the digital identity system (Davies, 2006), as is the case for the first version of eIDAS. Mutual recognition can be reached through accreditation and certification processes (ITU, 2014). *Harmonization* goes one step further and mandates the implementation of a similar set of rules, procedures, vocabularies or technical designs (e.g., digital wallets within the upcoming European Digital Identity Framework (Weigl, Amard, et al., 2022)).

Interoperability enablers: this dimension describes the choice to be made with regards to the reuse of building blocks produced by the community. Use of technical, organizational or semantic *standards* (e.g., OpenID Connect) can facilitate a harmonization approach. *Certification or accreditation mechanisms* are common means to achieve mutual recognition (e.g., the eIDAS certification). Finally, *open-source software* can also enable technical and semantic interoperability by virtue of common APIs (e.g., MOSIP implementation in Morocco, Ethiopia, Togo, Madagascar). A subset of these community resources is the *digital public good* standard, which can apply to both open-source software and open standards and testifies of some additional qualities such as their use of licenses approved by the Open Source Initiative (OSI). Both open-source software and the use of open standards are increasingly required in public tenders for digital identity infrastructure for their desirable properties, such as enabling interoperability (Almeida et al., 2011), and avoiding vendor lock-in (Medaglia et al., 2022). Open-source software used in the context of digital identity infrastructure includes the Modular Open Source Identity Platform (MOSIP), Open Civil Registration and Vital Statistics (OpenCRVS) and X-Road. Technical, organizational and semantic standards comprise, among others, those drafted by the European Telecommunications Standards Institute, the National Institute of Standards and Technology and the World

Wide Web Consortium (ENISA, 2023; ETSI, 2021; Grassi et al., 2017; Mittal, 2022; Sporny et al., 2019; W3C, 2022a).

Roles of private sector actors: while institutional actors are always involved in the supervision or the orchestration of the infrastructure and in the certification of digital identity data, the private sector can be authorized to take part in the provision and use of digital identity services in different ways. *No role* means that the digital identity system is seen as a purely public service for government to government, citizen to government and government to citizen use cases, and is fully delivered by the public sector with no involvement from the private sector. *Identity consumption* refers to the authorized usage of digital identity-related services such as identification and authentication during service delivery activities by private sector actors (e.g., through SingPass's MyInfo service in Singapore). *Identity provision* is a role that can take several forms, such as providing trusted data for use within the digital identity infrastructure (e.g., Banks in Sweden acting as an authoritative source), or issuing credentials (e.g., Buypass in Norway). *Registrar* is the role tasked with collecting and verifying identity data (e.g., PostIdent in Germany, some Aadhaar registrar / enrolment agencies in India). Finally, *infrastructural provision* relates to the technical roles that are necessary for the infrastructure to function, such as authentication and federation, certificate signing, PKI, identity access management, wallet provision (e.g., LuxTrust, Namirial, Idemia, Thalès). The choices to be made within dimension have been subject to intense scrutiny by policymakers and the civil society. Several failures and criticism have originated from the role of private sector actors, including the failure of the 2021 Swiss referendum on the Electronic Identification Services Act (Swiss Federal Counsel, 2021) and the rebuke from the Comptroller and Auditor General of India for the inappropriate governance of private sector actors within the Aadhaar ecosystem (CAG of India, 2021).

4.3. Funding management layer

The funding management layer is composed of two dimensions: **development funding** and **operational financing**.

Development funding: describes the infrastructure's funding model for the pre-operational phase. The characteristics are *public funding* (including loans from e.g., multilateral development banks such as the European Investment Bank), *public-private funding* (e.g., a build-operate-transfer agreement), a means often used in developing countries to reduce the upfront investment required from public bodies (Gelb & Diofasi, 2018), and *grants* (e.g., from donor organizations such as the World Bank's International Development Association). Development finance institutions have increasingly recognized the infrastructural aspect of digital identity and its enabling role for development outcomes (DPGA & GiZ, 2022; UNDP, 2023; World Bank, 2022b). Financing for digital identity infrastructure projects is now commonly available for LMIC countries. For example, the World Bank is particularly active in the ECOWAS region, providing a mix of grants and loans to Benin, Burkina Faso, Niger, Togo, Guinea and Côte d'Ivoire through their West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program, but also on other continents such as the Philippines, totaling more than $2,3bn in financing (World Bank, 2023b). On the other hand, private sector actors have also tailored their offering to emulate public-private partnerships found in physical infrastructure development, limiting the initial investment required by public authorities in the process (GSMA et al., 2016; IDEMIA, 2020).

Operational financing: relates to the financing of the operational phase. It targets financial sustainability of operations, including providing a return on investment to private partners who invested in the building of the capacity, when applicable. The main characteristics are *public budget* (e.g., in Thailand where transactions are free of charge for users and relying parties), *charge for relying parties* (e.g., in Peru where the private sector is charged for identification transactions (Reuben & Carbonari, 2017) or in Tanzania where NIDA charges Tshs 500 per identification transaction (Bhandari et al., 2021)), and *charge for data subjects* (e.g., issuance of a LuxTrust authentication token in Luxembourg). When charging back to relying parties, one key consideration is whether the public and private sector (when applicable) are charged the same amount. In many cases, such as in India and Argentina, identification and authentication transactions are free for the public sector, but not for the private sector (ID4D, 2019). In specific cases, *other* sources of revenue can come into play, such as revenues from licenses fees for access to authentication services (e.g., e-KYC User Agencies in India) or interests (e.g., accrued through the use of the UIDAI fund in India).

4.4. Data management layer

The data layer is composed of three dimensions: **data presentation model**, **identity matching approach** and **identity data storage**. Design decisions related to this layer directly impact data protection and privacy, and as such are often the subject of much scrutiny both from data protection authorities and citizens (Beduschi, 2021).

Data presentation model: identity data, in the form of attributes or bundled in credentials, can be presented for identification or authentication through different actors. *Identity provider to relying party*: the relying party retrieves identity information directly from the identity provider or the authoritative source (e.g., healthcare providers requesting data to social security entities). *Federation through one actor*: federation refers to the capacity to use the same identity information to access multiple services (Kallela, 2008). In the case of a single-actor federation model, a singular gateway allows for the exchange of data and oftentimes acts as an authentication provider (e.g., Aadhaar in India). *Federation through multiple actors*: several actors can act as federation service providers (e.g., FranceConnect in France). This model gives more choice to users and limits the consolidation of data and power within a single entity. *Data subject to relying party,* also sometimes called 'self-sovereign identity' (Pöhn et al., 2021): the data subject holds a digital credential which is directly shared with the verifier (relying party), without the involvement of an identity provider in the data exchange (e.g., the NDI in Bhutan). This data delivery method has recently come to the limelight, with digital health credentials having been used extensively during the COVID pandemic (Lacity & Carmel, 2022). In addition, the crystallization of technical standards such as decentralized identifiers (W3C, 2022a) and verifiable credentials (W3C, 2022b) have fostered their appropriation for more foundational identity management practices, as exemplified in Bhutan and in Europe by the recent revision of the eIDAS regulation. But despite this recent advance, in almost all cases today, the issuer of digital identity attributes or credentials is still taking part in a data presentation transaction, either by directly sending the data to the relying party or by acting as a federation provider, such as in India.

Identity matching approach: linking of identity data, or identity matching, can take two main governance configurations. Identity data matching can either be *mediated* by a third-party (e.g., the sourcePin Register Authority in Austria), or *non-mediated* (e.g., through a unique identifier, technological means, or simply comparing datasets for common attributes). Mediation techniques can be witnessed in several HICs with a high level of data privacy awareness and concern, such as in Austria, in Estonia, in Belgium and in the Netherlands, where a translation service matches data only in authorized cases, without revealing a general identifier for the person. This is often not the case in LMICs, where a unique identification number is used as a basis for identification (e.g., the National Identification Number in Nigeria). It is also sometimes seen as a condition for funding disbursement by funding agencies, such as in the case of WURI (World Bank, 2018).

Trusted sources: data pertaining to digital identity transactions can be stored with different actors. It is important to note that this data does not exclusively consist of identity attributes. Certificate revocation information (Sedlmeir et al., 2021) and issuer public keys (Lacity & Carmel, 2022) are prime examples of data required to ensure the authenticity, integrity and validity of identity attributes and credentials. Data can be stored in *government-controlled databases* (e.g., biographic and biometric data within Aadhaar in India). *User wallets* can also act as a trusted source, by storing verifiable credentials and electronic attestations of attributes (e.g., the European Digital Identity Wallet), allowing data subjects to hold a trusted version of their identity data. These wallets can take several forms, from smartphone applications to simple file storage on a computer. Finally, *distributed ledgers* can also play a role in storing trusted data, with the primary use cases being registers of issuers, public keys of issuers, registry of schemas, and certificate revocation lists (e.g., a possible usage of the European Blockchain Services Infrastructure within the European Digital Identity Framework (EBSI, 2023)). When the trust placed in the data does not originate from the government, trust can be achieved through different means. In the case of the digital wallet, trust is mainly anchored in cryptography and organizational processes, linked to the verifiability of credentials stored within them (Sedlmeir et al., 2021). In the case of distributed ledgers, consensus mechanisms combined with immutability and transparency can act as the root of this trust (Haddouti & Ech-Cherif El Kettani, 2019). In most cases involving user wallets, a copy of the data also remains in a repository to mitigate issues linked to credential loss and enable legitimate use by government without the express consent and action of the citizen.

5. ‘In-situ’ discussion: interpreting our findings through instantiations of the taxonomy - the case of India

In the previous section, we presented the final taxonomy and guided its reading in an explanatory manner, focusing on detailing and making sense of the input gathered during our seven iterations. In this section, we provide some keys for its interpretation using both theoretical and empirical evidence, helping us answer our second research question. Doing so, we surface the implications of our findings, both highlighting their practicality and opening the conversation on their significance.

First, we present a possible instantiation of the taxonomy, giving a high-level overview of a single case. Given the breadth and complexity of digital identity infrastructures, we would expect a typical research project to focus on at most one or two layers, in order to give it the depth of analysis it deserves (see e.g., Klitgaard, (2011)). Alternatively, focusing on one specific dimension with a comparative approach could similarly yield interesting analytical frames. In this example, we select the Indian Aadhaar case, for it is arguably the most researched and well-known digital identity infrastructure in a LMIC today, giving an appropriate point of reference for our readership, but any other digital identity infrastructure could be used with this format. It is also a particularly interesting, multifaceted case that has embraced a wide diversity of approaches over the years, showcasing how governance aspects of an infrastructure can evolve over time. While the name *Aadhaar* technically refers to the 12-digit identification number issued by the Unique Identification Authority of India (UIDAI), it is also extensively used for the infrastructure that supports it, a usage that we will also adopt here for simplicity purposes. In this example, we do not aim to provide an exhaustive analysis of the dynamics at play. Instead, our objective is to highlight how the taxonomy can be used with a specific analytical lens to uncover and apprehend topics of relevance for both researchers and practitioners.

5.1.1. Institutional arrangement

Authority governance model: The Indian implementation presents an interesting case with regards to governance model evolutivity. At the behest of an Empowered Group of Ministers (a group of Indian government ministers empowered to investigate, report on and make decisions on a particular matter of interest), the Unique Identification Authority of India (UIDAI) was initially established in January 2009 as an executive authority. It was anchored in India's Planning Commission (DoIT India, 2011), an institution tasked with elaborating five-year plans for the country with comparable powers to a ministry: while the Prime Minister was its Chairman, the Deputy Chairman had the rank of a full Cabinet Minister (President's Secretariat, 1979). However, despite being comparable to a ministry, the Planning Commission was a transversal government institution, which reinforced the transversal character of the role of the UIDAI. Digital identity was arguably already seen as a general government service as opposed to the prerogative of a more functional ministry – after all, Aadhaar means 'foundation' in many languages used in India. At its creation, it was decided that its governance model could be reviewed at an appropriate time, with the group of ministers already considering making it more autonomous as a statutory authority (UIDAI, 2010). This change of status from a *ministerial entity* to a *fully autonomous entity* took place in 2016 with the *Aadhaar Act* (2016) which granted it the supervisory / autonomous body status despite being under the Ministry of Electronics and Information Technology (IGOD, 2023).

Evolution over time was also seen within the *additional authority prerogatives* dimension. Sarkar (2014) hypothesized that the original anchoring of UIDAI to the Planning Commission was due to the future database that UIDAI would foresee the development of, would become an important tool for planners, citing the DoIT India report (2011): ‘The existence of such a data base along the length and breadth of the country will impart a new direction to the overall governance […] by better planning of infrastructural requirements as the count of people residing in an area would be known at any point of time’. But this prerogative collation wasn’t the only one: originally, the Empowered Group of Ministers considered UIDAI to hold the responsibility of managing both digital identification capabilities and the national population register (UIDAI, 2010), thus linking the prerogatives of *civil registration* to that of digital identification. In its current form, the UIDAI’s objective is to facilitate the delivery of subsidies, benefits and services (*Aadhaar Act*, 2016), however its role in reaching this objective limited to ‘assigning unique identity numbers [to individuals residing in India] and for matters connected therewith or incidental thereto’, and thus is *solely concerned with digital identification*. This institutional arrangement is well-aligned with its intended neutrality and transversal role, but less so with its stated objective (delivery of subsidies, benefits and services) which involves a much more social orientation. This discrepancy between stated intent and governance decision could simply be fortuitous. But, borrowing from Masiero's (2018) piece on trust-building in Aadhaar and Khera's (2017) observation that Aadhaar had a limited role in its stated welfare objective, one could hypothesize that this framing of Aadhaar as a program with a social objective was actually designed as a trust-building tool as opposed to a genuine program direction. We leave these hypotheses to be tested by other researchers: in this piece, we will be content with simply highlighting the hypothesis-building quality of contextualizing the taxonomy.

5.1.2. Ecosystem management

The *Aadhaar Act* (2016) clearly stipulates that the *subjects* of the infrastructure are *residents*, thus including the categories of *nationals (residents)*, *non-nationals (residents)* and *persons without proof of legal identity*, should they be residents in India. This naturally raised the question of non-resident Indians (NRI), given that an Aadhaar number was de facto needed for some administrative procedures. This category of subjects needed to have stayed 182 days or more within the past 12 years before being eligible, generating obvious issues with service provision. In response, this dimension was extended to also include *nationals (non-residents)* in 2019 (UIDAI, 2019a). But choices made within this dimension could have been quite different: amendments made in 2004 to the *Citizenship Act (1955*) opened the door to the issuance of multipurpose identity cards to Indian *citizens,* which could have served as a basis for identification and authentication, on top of being a proof a citizenship.

Despite the actualization of its expected benefits requiring integration with the practices or local bureaucracies (Madon et al., 2022), Aadhaar is primarily concerned with the *national geographical scope*, and thus does not yet have a particular interoperability approach at the sub-national or international level. It does, however, serve as an interoperability layer between different services at the national level and relies on standards, certification mechanisms and open-source software, which might ease a potential future process of expanding geographical scope. Areas where standards are used include biometrics (e.g., ISO/IEC 19794, Information Technology - Biometric data interchange formats) and authentication (Open ID Connect implemented as part of the e-Pramaan gateway). Aadhaar also makes use of certification mechanisms: as an example, certification is a prerequisite for obtaining the authorization to act as a registrar (UIDAI, 2022c). An interesting combination of standards and certification regulate biometric capabilities in Aadhaar. Indeed, the UIDAI created standards where they didn’t exist (e.g., for iris scanners) and applied them through a certification process: only those companies who could meet the standard would be allowed to perform biometric operations for the system (Gelb & Clark, 2013). Open-source software is also widely used, with MySQL, Apache Hadoop and RabbitMQ being three examples credited with helping address the important scalability and data management challenges of running Aadhaar while avoiding vendor lock-in (Varma, 2010).

Finally, the *role of private sector actors* within Aadhaar has been an important point of contention between institutional actors and the civil society. Although the private sector also plays *infrastructural roles* (e.g., biometric matching system provider), we will here highlight two aspects exemplifying the need to assess the choices made within this dimension: the role that private sector actors have played as *registrars* and as *identity service consumers* (note: while the UIDAI makes a distinction between registrars and enrolment agencies, the former being tasked with planning and the latter with execution of enrolment, we consider them here as parts of the same function and will use the term registrar).

From the early stages, the UIDAI identified enrolment as one of the key risks of the project, and in particular with regards to reaching the target population. To address this risk, the UIDAI took the decision to build their enrolment approach through partnerships with existing infrastructure of government as well as private sector actors (UIDAI, 2010). Registrars were initially given flexibility regarding pricing, although strict rules have since been issued on how much a registrar can charge for an Aadhaar-related transaction (Aadhaar policy on pricing, 2020). But in a context when not being enrolled means substantial difficulties in accessing welfare, a clear power imbalance between registrars and residents led to abuse. For example, some residents were charged for services that were supposed to be free (Press Information Bureau, 2017). The level of fraud was such that in March 2023, UIDAI announced that 1.2% of all enrolment operators had been suspended in the last 12 months (Press Information Bureau, 2023). This short analysis from a single characteristic already yields many important research questions: would these fraud cases have occurred if the private sector had not been involved in enrolment? Would objectives in terms of population coverage still have been attained? What, then, should drive the decision to allow the private sector to take on a registrar role?

The second role worth highlighting in this case is the one of identity consumption. Aadhaar's initially stated objective was to provide for 'good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services' (*Aadhaar Act*, 2016). The addition of section 57 of the Act, opening the use of Aadhaar for 'any purpose' by 'any corporate body or person' seems counter to this initially stated objective. Despite this, private sector companies started requiring identification through Aadhaar to grant access to their services. This was eventually struck down as unconstitutional by the Supreme Court of India in its 26 September 2018 verdict: only specific private sector users such as banks were then allowed to use Aadhaar for the purpose of fighting against money laundering and tax evasion, under the provisions of the Prevention of Money Laundering Act of 2002. But in 2023, history seemed intent on repeating itself, with a proposal legally opening the use of Aadhaar authentication to the private sector once more (Ministry of Electronics and IT, 2023). This simple example serves to highlight the value in researching how the role of the private sector affects the interplay between governance arrangements, legislation and targeted objective of the infrastructure, and the impact of a misalignment thereof.

5.1.3. Funding management

Aadhaar was conceived as a public infrastructure primarily targeting inclusion and more efficient delivery of welfare services (UIDAI, 2010), and as such its original funding came from the public sector. In 2012, the National Institute of Public Finance and Policy estimated that an 56% internal return rate could be reached within 10 years, a significant return on investment to be accrued thanks to the 'reduction of leakages occurring due to identification and authentication issues' (NIPFP, 2012). However, despite taking on a significant part of the development of the infrastructure, the UIDAI sought ways to reduce investment costs by leveraging *public-private partnerships* models. Enrolment and data update capabilities, and biometric identification and deduplication capabilities, present two examples in this regard. From very early on, it was assessed that relying on the private sector was necessary to reach sufficient coverage of India's territory and closeness to its population (UIDAI, 2010). A governance arrangement was thus developed, consisting in granting registrar / enrolment providers the necessary authorizations to perform enrolment and update of identity data. These actors would be remunerated per transaction. Regarding biometric operations, a similar governance model was set in place, whereby only certified companies could provide biometric services, who would then be paid by transaction. This shift from investment costs to transaction costs can be credited for limiting the initial investment required. However, it hasn't gone uncriticized, especially in its application. The Comptroller and Auditor General of India identified several areas where the contractual conditions and their application were too lenient for the private sector and ended up being more costly to the government than they should have been

(CAG of India, 2021).

As regards *operational funding*, the Aadhaar infrastructure is still predominantly funded by governmental grants: in 2022, 72% of its revenues came from grants and subsidies, while 22% was income from service provision, and the remaining 6% from other sources such as license fees and interests on bank deposits (UIDAI, 2022a). Out of the service provision revenues, 73% originated from *charges to relying parties* (authentication services and license fees), 23% from *charges to data subjects* (e.g., data update, ordering a PVC Aadhaar card) and 4% from *other incomes*. Authentication fees were reduced by 85% in 2021 from ₹20/- to ₹3/- per transaction (from ~USD 0.24 to 0.036), and even to ₹1/- (~USD 0.012) for telecommunication operators, in order to 'expand Aadhaar usage' (UIDAI, 2022a). A careful balance, well depicted in this succinct example, must be found within this dimension. Increasing the cost of service may well help generate revenues for sustainability, but at the risk of reducing the affordability of infrastructure usage, reducing its capacity to deliver wider societal benefits.

5.1.4. Data management

Aadhar provides an interesting example of diversification in data presentation models. Indeed, the infrastructure can both act as a *singular federation service* between users and service providers and also as an *identity provider sharing data with relying parties*. It also supports the generation and usage of so-called offline e-KYC files (UIDAI, 2023a), effectively allowing *data subjects to directly share their identity data with relying parties* in a verifiable manner. The federation service is the historic and primary capability of the Aadhaar infrastructure. It allows data subjects to authenticate themselves to service providers (called authentication user agencies). To do so, the data subject is required to provide their Aadhaar number and some biographic, or/and biometric information, which are then submitted along with the data subject’s consent to the Central Identities Data Repository for verification (UIDAI, 2023b). The service provider subsequently receives a yes/no response, used as a basis to grant access to the requested services. This data presentation model is helpful when only an authentication of a data subject is required. An extension of this capability is the e-KYC process, through which service providers can access verified identity information stored in the Aadhaar database (UIDAI, 2019b). This model eases the challenge of getting access to verifiable identity information and reduces the risk of data duplication or data inaccuracies due to manual entry. Finally, this e-KYC process can be performed offline as well: a data subject can download an XML file containing their identity information in an encrypted format, which they can then share with a service provider directly without the transaction having to be validated by the central infrastructure. This model is particularly helpful in cases when internet network connectivity is not guaranteed. As suggested by these three examples, broadening the diversity of presentation models can help accommodate the requirements and the context of both data subjects and data providers looking to benefit from the infrastructure.

Within the Aadhaar infrastructure, *identity matching* can take place both in a *mediated* and a *non-mediated* way. The Aadhaar number being a unique 12-digit number, it can effectively be used as such to match identity data by simple means of comparison, representing a significant privacy risk. In response, the UIDAI developed a tokenization mechanism, allowing data subjects to generate ‘Virtual IDs’ and mandate the use of a specific, service provider-specific identifier as opposed to the general Aadhaar number for certain relying parties (local authentication and e-KYC agencies) (UIDAI, 2018). The Aadhaar infrastructure is then required to translate these tokenized identifiers when data matching is necessary, acting as a mediating agent. This example shows how two identity matching approaches can co-exist. While one enables accuracy and ease of use due to its uniqueness and generality, the other provides higher privacy at the cost of technical and organizational complexity. In the case of the Virtual ID, a higher level of digital literacy is also required, which can limit the actualization of its benefits.

With regards to *trusted data sources*, Aadhaar primarily relies on its own databases, where biometric and biographic data is stored. When necessary, it also makes the link between authoritative sources, acting as a gateway between a source and a relying party (UIDAI, 2022b). This trusted data can also be decentralized with data subjects as an XML file for them to store in a digital wallet. Distributed ledgers have not yet been used in the Aadhaar infrastructure, although it has been mentioned as a potential use case by the Policy Commission of India, the responsible for providing 15- and 7-year road maps and strategic plans for India (NITI Aayog, 2020).

5.1.5. Summary of governance choices within the Aadhaar infrastructure

This depiction in broad strokes of the Aadhaar example, viewed from the lens of our taxonomy, allowed us to exemplify through a concrete case how the key governance decisions become operationalized in a digital infrastructure, to highlight some of the dynamics influencing these choices, and to postulate some of their impacts. Below, we propose a simplified visualization of this case. This mapping represents a quickly understandable profile of a case that can be used for comparison purposes and for hypothesis building. This can be used by practitioners to quickly evaluate how their implementations compare to their peers', and by researchers for developing additional analytical layers, such as studies of archetypical implementations.

Strategic Institutional and Governance Choices for Digital Identity Infrastructure

Layer	Dimension	Characteristics				
Institutional Arrangement	**Authority governance model** *(mutually exclusive)*	Inter-ministerial entity	Ministerial entity	Semi-autonomous entity (with stakeholder representation)	Fully autonomous entity (with direct Cabinet- or Executive-level reporting)	
	Additional authority prerogatives	Civil registration	Identity document and certificates issuance	Others (e.g. statistics, digitalization strategy)	Single purpose authority	
Ecosystem Management	**Subjects**	Nationals (residents)	Nationals (non-residents)	Non-nationals (residents)	Non-nationals (non-residents)	Persons without proof of legal identity
	Geographical scope	Sub-national		National		Transnational
	Interoperability approach	None		Mutual recognition		Harmonization
	Interoperability enablers	Standards (technical, organizational, semantic)		Certification or accreditation mechanisms		Open-source / community software
	Roles of private sector actors	None	Identity consumption	Identity provision	Registrar	Infrastructural provision
Funding Management	**Development funding**	Public funding		Public-private partnership		Grant
	Operational financing	Public budget	Charge for relying parties	Charge for data subjects	Other	
Data Management	**Data presentation model**	Identity provider to relying party	Federation through 1 actor	Federation through multiple actors	Data subject to relying party	
	Identity matching approach	Mediated		Non-mediated		
	Trusted sources	Government-controlled databases		Digital wallets		Distributed ledgers

Table 4. Mapping of the Indian case within the taxonomy (the light grey colouring highlights the characteristics of the case).

6. Discussion

While this list of dimensions and characteristics can give the impression that infrastructure designers have complete choice over their design, several important parameters can dictate the decisions that are available to them. A typical example would involve the legacy arrangements in place. Indeed, making impactful design decisions that imply reworking existing processes and governance agreements often entail high financial and time investments. This is particularly the case when new legislation needs to be enacted. In addition, while digital identity might currently be at the top of the agenda for many countries worldwide (G20, 2023), it is not necessarily the case everywhere. The attention of policymakers is limited, and the level of ambition for digital identity infrastructure might be impacted by micro- and macro-level political considerations, such as the proximity to elections. Many other factors naturally come into play in the decision process, such as culture, economic, geographic and demographic situation among others. Decisions, then, are clearly driven by context, and their appropriateness subject to interpretation (Madon, 2015).

Agreeing with this perspective, we aimed to guide our reader and provide nuance as to the interpretation of these choices within a particular context. We did so by looking at the different dimensions of the taxonomy within the Indian Aadhaar case, and through the lens of the main challenges facing LMICs that are pervasive in practitioners' discourses, the analyzed literature and archival records. Doing so, we provided answers to the research questions of this paper. Several implications are drawn from our results, applicable for both theory and practice.

Our work contributes to theory through a richer understanding of the yet under-researched field of governance of digital identity infrastructure. The taxonomy expands the existing body of knowledge through a consolidation of practitioners and academic insights and establishes a consensus-based terminology to support a common understanding on this topic. By providing a set of unifying constructs supporting interpretation of aspects of relevance in our area of interest, this taxonomy can serve as a framework allowing generalization, communication and application of findings (Glass & Vessey, 1995). This contribution is of value to e-government research on digital infrastructure (Janowski, 2015) and can support other research directions within the wider information systems domain at large (Belanger & Carter, 2012). In brief, the contributed taxonomy can be used to distinguish and depict strategic governance aspects of digital identity infrastructures in a systematic and comprehensive way, and serve as contextualization basis for hypothesis-making (Glass & Vessey, 1995) and theory-building (Bapna et al., 2004).

Our instantiation helped bring to light some of these qualities. While their depiction is more valuable in their context, and we will thus refrain from making a summary here, we can highlight that many of our hypotheses revolved around the appropriateness of certain decisions in a specific context, and the interplay between them. Among the stand-out topics were considerations linked to arrangements with the private sector, which pervaded a significant part of the taxonomy. This instantiations also helped us raise many questions that would deserve attention in future research, in particular concerning the impact that governance choices can have on actualization of digital identity infrastructure benefits. Empirical comparative research approaches would be particularly appropriate here, generating relevant theory and bringing actionable results to be leveraged by the practitioner community.

We contribute to practice on three levels. First, the list of governance characteristics of digital identity infrastructure, along with relevant design choices, can help practitioners during the design and implementation of such infrastructure. Second, given the concise and explanatory character of the provided taxonomy, we provide policymakers with a practical tool for contextualization to better assess the design choices that they are faced with (Janowski, 2015), thus also answering the call for better research and training resources in the area of digital identity (Wimmer et al., 2020). We reinforce this contribution by giving two complementary examples of possible instantiations of the taxonomy, concretely showcasing how the taxonomy's analytical frame can be leveraged in practice. Third, citizens who are impacted by the deployment and use of digital identity infrastructure are provided with a tool to concisely apprehend their impactful governance characteristics. This can help citizens make better informed decisions and enable them to steer the design of these features through participative action. It also supports approach uniformity when it comes to successful digital identity infrastructure evolution.

Some limitations of this research must also be acknowledged. When dealing with a taxonomy, one must remember that they do not hold truth value, nor do they intend to (Iivari, 2007). Although we contend that it is useful as a tool, and hope that we were able to demonstrate how, this taxonomy is necessarily imperfect. A few reasons explain this, aside from those inherent to the nature of taxonomies. First, the field of digital identity infrastructure is still relatively nascent and, coupled with the accelerating pace of technological innovation in the realm of identity management, it is likely that this taxonomy will have to be extended in the medium-term. Second, the high level of complexity of the topic should lead us to remain humble about the universal character of the taxonomy, as its focus might have been steered in part by the current challenges facing the digital identity community. Indeed, some of the strategic governance choices facing institutional actors today might evolve, and new governance choices might soon need to be considered in a different light. We must also recognize that while the taxonomy made sense to our interview partners, the topic at hand is particularly complex and can be challenging to understand by people less acquainted with the field of digital identity. Finally, while two of our iterations consisted in an analysis of a representative sample of instantiations of digital identity infrastructure, a systematic, transversal evaluation of further existing instantiations could potentially reveal rare characteristics that would deserve to be added.

These limitations lead us to call for further research. To better assist practitioners with actionable knowledge that can be applied within their specific context, case-study based evaluations of the impact resulting from governance decisions could yield significant insights. While we focused on the governance aspects of digital identity infrastructure, there would also be value in delving into the technical elements that compose the infrastructure and the interplay between these two domains. Finally, there is an opportunity to dig deeper into each of the dimensions of the taxonomy, bringing in a more focused and granular view beyond the strategic design choices. Future research could also adopt a reverse innovation frame (Immelt et al., 2009), looking at how innovation originating from developing countries could make an impact on challenges in HICs.

7. Concluding remarks

Digital identity infrastructures have seen a rise in interest from governments wanting to enable participation of their citizens in a digital society and economy. However, on the one hand recent experiences show that misaligned organizational and institutional arrangements can cause project failures even in rich, developed countries, leading to public distrust, and wasted resources. On the other hand, a heightened vulnerability to adverse effects concerns low- and middle-income countries, for which the relative costs of a digital identity infrastructure are higher and the expected benefits substantially more transformative. To overcome this challenge and limit the risks of project failure, strategic governance choices of digital identity infrastructure design must be well identified, understood, planned, and communicated. A taxonomy can be a powerful tool to support this objective, thanks to its ability to structure and organize the body of knowledge (Glass & Vessey, 1995). We thus developed a taxonomy of strategic governance choices for digital identity infrastructures following the development process proposed by Nickerson et al. (2013). This systematic process resulted in a final taxonomy consisting of 4 layers, 12 dimensions and 43 characteristics of governance decision domains in digital identity infrastructure. In order to demonstrate its interpretive qualities, guide future users of the taxonomy, and provide a discussion basis for its implications, we also instantiated the taxonomy using a case approach.

When well designed and implemented, digital identity infrastructures have the potential to promote economic development and socioeconomic inclusion in the digitalized world. Building on the outcome of our research, future research may contribute to the successful actualization of these benefits.

8. Appendix

ID	Interviewee's position	Iteration	Category	Years of experience in digital identification
1	Practitioner	2	LMIC	14
2	Practitioner	2	HIC	10
3	Practitioner	2	LMIC	11
4	Practitioner	2	HIC	21
5	Practitioner	2	HIC	7
6	Practitioner	2	LMIC	13
7	Practitioner	2	HIC	6
8	Practitioner	2	HIC	10
9	Researcher	3	Global	14
10	Researcher	3	Global	2
11	Researcher	3	Global	3
12	Researcher	3	Global	2
13	Practitioner	6	LMIC	9
14	Practitioner	6	Global	4
15	Practitioner	6	Global	4
16	Practitioner	6	LMIC	5
17	Practitioner	6	LMIC	9

Table 5. Overview of interviewees

9. References

50-in-5. (2023). *Implementing digital public infrastructure, safely and inclusively*. 50-in-5. https://50in5.net/

Aadhaar Act. (2016). https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

Abraham, S. (2020). *Building Trust : Lessons from Canada's Approach to Digital Identity*. https://www.orfonline.org/research/building-trust-lessons-from-canadas-approach-to-digital-identity-67360/

Addo, A., & Senyo, P. K. (2021). Advancing E-governance for Development : Digital Identification and its Link to Socioeconomic Inclusion. *Government Information Quarterly*.

AlBdairi, A. J. A., Xiao, Z., Alkhayyat, A., Humaidi, A. J., Fadhel, M. A., Taher, B. H., Alzubaidi, L., Santamaría, J., & Al-Shamma, O. (2022). Face Recognition Based on Deep Learning and FPGA for Ethnicity Identification. *Applied Sciences*, *12*(5), Article 5. https://doi.org/10.3390/app12052605

Almeida, F., José, O., & José, C. (2011). Open Standards And Open Source : Enabling Interoperability. *International Journal of Software Engineering & Applications*, *2*. https://doi.org/10.5121/ijsea.2011.2101

Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy*, *3*, e35. https://doi.org/10.1017/dap.2021.35

Antonio, A., & Tuffley, D. (2014). The Gender Digital Divide in Developing Countries. *Future Internet*, *6*(4), 673-687. https://doi.org/10.3390/fi6040673

Ari, I., & Koc, M. (2018). Sustainable Financing for Sustainable Development : Understanding the Interrelations between Public Investment and Sovereign Debt. *Sustainability*, *10*(11), Article 11. https://doi.org/10.3390/su10113901

Australian Government. (2023). *Trusted Digital Identity Framework (TDIF) | Digital Identity*. https://www.digitalidentity.gov.au/tdif

Bailey, K. D. (1994). *Typologies and taxonomies : An introduction to classification techniques*. Sage.

Bannister, F. (2005). The panoptic state : Privacy, surveillance and the balance of risk. *Information Polity, 10*(1,2), 65-78. https://doi.org/10.3233/IP-2005-0068

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government : A framework and programme for research. *Government Information Quarterly, 31*(1), 119-128. https://doi.org/10.1016/j.giq.2013.06.002

Bapna, Goes, Gupta, & Jin. (2004). User Heterogeneity and Its Impact on Electronic Auction Market Design : An Empirical Exploration. *MIS Quarterly, 28*(1), 21. https://doi.org/10.2307/25148623

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-Sovereign Identity : Use-cases, Technologies, and Challenges for Industrial IoT. *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1173-1180. https://doi.org/10.1109/ETFA.2019.8869262

Beduschi, A. (2019). Digital identity : Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society, 6*(2), 205395171985509. https://doi.org/10.1177/2053951719855091

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies : Data privacy and human rights considerations. *Data & Policy, 3*. https://doi.org/10.1017/dap.2021.15

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165-176. https://doi.org/10.1016/j.jsis.2007.12.002

Belanger, F., & Carter, L. (2012). Digitizing Government Interactions with Constituents : An Historical Review of E-Government Research in Information Systems. *Journal of the Association for Information Systems*, *13*(5), 363-394. https://doi.org/10.17705/1jais.00295

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790. https://doi.org/10.1016/j.cose.2020.101790

Bhandari, V., van der Spuy, A., Trikanad, S., & Tshering Paul, Y. (2021). *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa : Comparative Analysis of Findings from Ten Country Case Studies (Research ICT Africa and the Centre for Internet & Society)* (SSRN Scholarly Paper 3969781). https://doi.org/10.2139/ssrn.3969781

Bhatia, A., Donger, E., & Bhabha, J. (2021). 'Without an Aadhaar card nothing could be done' : A mixed methods study of biometric identification and birth registration for children in Varanasi, India. *Information Technology for Development*, *27*(1), 129-149. https://doi.org/10.1080/02681102.2020.1840325

Bhatt, P., Moulton, S., & Sutterlin, E. (2021). *Identified but Unheard—Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities*. https://www.ndi.org/sites/default/files/Identified%20but%20Unheard%20FINAL.pdf

Blakstad, S., & Allen, R. (2018). Leapfrogging Banks in Emerging Markets. In S. Blakstad & R. Allen, *FinTech Revolution* (p. 121-132). Springer International Publishing. https://doi.org/10.1007/978-3-319-76014-8_7

Bocchini, P., Frangopol, D. M., Ummenhofer, T., & Zinke, T. (2014). Resilience and Sustainability of Civil Infrastructure : Toward a Unified Approach. *Journal of Infrastructure Systems*, *20*(2), 04014004. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000177

Bodó, B. (2021). Mediated trust : A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668-2690. https://doi.org/10.1177/1461444820939922

Bratton, M., & Gyimah-Boadi, E. (2016). *Do trustworthy institutions matter for development ? Corruption, trust, and government performance in Africa*. https://www.afrobarometer.org/wp-content/uploads/migrated/files/publications/Dispatches/ab_r6_dispatchno112_trustworthy_institutions_and_development_in_africa.pdf

CAG of India. (2021). *Report of the Comptroller and Auditor General of India on the Functioning of Unique Identification Authority of India*. https://cag.gov.in/webroot/uploads/download_audit_report/2021/24%20of%202021_UIDAI-0624d8136a02d72.65885742.pdf

Carmody, P. (2020). Eprint of Dependence not Debt Trap Diplomacy. In *Area Development and Policy* (Vol. 5). https://doi.org/10.1080/23792949.2019.1702471

Carter, L., & Weerakkody, V. (2008). E-government adoption : A cultural comparison. *Information Systems Frontiers*, *10*(4), 473-482. https://doi.org/10.1007/s10796-008-9103-6

Chudnovsky, M., & Peeters, R. (2021). A cascade of exclusion : Administrative burdens and access to citizenship in the case of Argentina’s National Identity Document. *International Review of Administrative Sciences, 88,* 002085232098454. https://doi.org/10.1177/0020852320984541

Cicchiello, A. F., Kazemikhasragh, A., Monferrá, S., & Girón, A. (2021). Financial inclusion and development in the least developed countries in Asia and Africa. *Journal of Innovation and Entrepreneurship, 10*(1), 49. https://doi.org/10.1186/s13731-021-00190-4

Citizenship Act, 1955. (1955). https://www.indiacode.nic.in/bitstream/123456789/1522/1/a1955-57.pdf

Cooper, I., & Yon, J. (2019). Ethical Issues in Biometrics. *Science Insights, 30*(2), 63-69. https://doi.org/10.15354/si.19.re095

Dahan, M., & Hanmer, L. (2015). *THE IDENTIFICATION FOR DEVELOPMENT (ID4D) AGENDA: Its Potential for Empowering Women and Girls*.

Davies, G. (2006). Is Mutual Recognition an Alternative to Harmonization? Lessons on Trade and Tolerance of Diversity from the EU. In L. Bartels & F. Ortino (Éds.), *Regional Trade Agreements and the WTO Legal System* (p. 0). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199206995.003.0012

Dawes, S. S. (2009). Governance in the digital age : A research and action framework for an uncertain future. *Government Information Quarterly*, *26*(2), 257-264. https://doi.org/10.1016/j.giq.2008.12.003

Diniz, E. H., Siqueira, E. S., & van Heck, E. (2019). Taxonomy of digital community currency platforms. *Information Technology for Development, 25*(1), 69-91. https://doi.org/10.1080/02681102.2018.1485005

DoIT India. (2011). *Compendium_FINAL_Version_220211(1).pdf*. https://www.meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211(1).pdf

Doty, D. H., & Glick, W. H. (1994). Typologies as a Unique Form of Theory Building : Toward Improved Understanding and Modeling. *The Academy of Management Review*, *19*(2), 230. https://doi.org/10.2307/258704

DPGA, & GiZ. (2022, mai). *GovStack Definitions : Understanding the Relationship between Digital Public Infrastructure, Building Blocks & Digital Public Goods*. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf

Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating the 'Troublemakers' : A taxonomy for cooperation between banks and fintechs. *Journal of Economics and Business*, *100*(C), 26-42. https://doi.org/10.1016/j.jeconbus.2018.04.002

EBSI. (2023). *EBSI's Credential Status Framework and how to choose a revocation method when using W3C Verifiable Credentials (and more)*.

Edelman. (2023). *2023 Edelman Trust Barometer*. Edelman. https://www.edelman.com/trust/2023/trust-barometer

ENISA. (2020). *eIDAS compliant eID solutions*.

ENISA. (2023). *Digital Identity Standards*. https://www.enisa.europa.eu/publications/digital-identity-standards

ETSI. (2021). *TS 119 461*. https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

European Commission. (2021, juin 3). *Commission proposes a trusted and secure Digital Identity for all Europeans* [Text]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

European Parliament. (2023). *10 2023 | A Europe Fit for the Digital Age | Revision of the eIDAS Regulation – European Digital Identity (EUid)*.

Feng, K., Wang, S., Li, N., Wu, C., & Xiong, W. (2018). Balancing public and private interests through optimization of concession agreement design for user-pay PPP projects. *Journal of Civil Engineering and Management*, *24*(2), Article 2. https://doi.org/10.3846/jcem.2018.455

Fitzgerald, B., & Kenny, T. (2004). Developing an information systems infrastructure with open source software. *IEEE Software*, *21*(1), 50-55. https://doi.org/10.1109/MS.2004.1259216

G20. (2023). *G20_Digital_Economy_Outcome_Document _and_Chair's_Summary_19082023.pdf*. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20_Digital_Economy_Outcome_Document%20_and_Chair%27s_Summary_19082023.pdf

Gavan, L., Hartog, K., Koppenol-Gonzalez, G. V., Gronholm, P. C., Feddes, A. R., Kohrt, B. A., Jordans, M. J. D., & Peters, R. M. H. (2022). Assessing stigma in low- and middle-income countries : A systematic review of scales used with children and adolescents. *Social Science & Medicine*, *307*, 115121. https://doi.org/10.1016/j.socscimed.2022.115121

Gelb, A., & Clark, J. (2013). *Performance Lessons from India's Universal Identification Program*. https://www.cgdev.org/sites/default/files/biometric-performance-lessons-India.pdf

Gelb, A., & Diofasi, A. (2018). *Identification Revolution : Can Digital ID be Harnessed for Development?*

Gelb, A., & Metz, A. D. (2018). *Identification Revolution : Can Digital ID be Harnessed for Development?* Brookings Institution Press. https://www.jstor.org/stable/10.7864/j.ctt21c4t40

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology : A survey. *International Journal of Network Management*, *32*(2), e2180. https://doi.org/10.1002/nem.2180

Giannopoulou, A. (2020). Data Protection Compliance Challenges for Self-sovereign Identity. In J. Prieto, A. Pinto, A. K. Das, & S. Ferretti (Éds.), *Blockchain and Applications* (p. 91-100). Springer International Publishing.

Giannopoulou, A. (2023). Digital Identity Infrastructures : A Critical Approach of Self-Sovereign Identity. *Digital Society, 2*(2), 18. https://doi.org/10.1007/s44206-023-00049-z

Gil-Garcia, J. R. (2012). *Enacting Electronic Government Success : An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions* (Vol. 31). Springer US. https://doi.org/10.1007/978-1-4614-2015-6

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020). Towards a comprehensive understanding of digital government success : Integrating implementation and adoption factors. *Government Information Quarterly, 37*(4), 101518. https://doi.org/10.1016/j.giq.2020.101518

Glass, R. L., & Vessey, I. (1995). Contemporary Application-Domain Taxonomies. *IEEE Software, 12*(4), 63-76. https://doi.org/10.1109/52.391837

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines : Revision 3* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

GSMA, World Bank Group, & Secure Identity Alliance. (2016). *Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

Gurara, D., Klyuev, V., Mwase, N., & Presbitero, A. F. (2018). Trends and Challenges in Infrastructure Investment in Developing Countries. *International Development Policy | Revue Internationale de Politique de Développement, 10.1*, Article 10.1. https://doi.org/10.4000/poldev.2802

Haddouti, S. E., & Ech-Cherif El Kettani, M. D. (2019). Analysis of Identity Management Systems Using Blockchain Technology. *2019 International Conference on*

Advanced Communication Technologies and Networking (CommNet), 1-7. https://doi.org/10.1109/COMMNET.2019.8742375

Hanna, R., & Olken, B. A. (2018). Universal Basic Incomes versus Targeted Transfers : Anti-Poverty Programs in Developing Countries. *Journal of Economic Perspectives, 32*(4), 201-226. https://doi.org/10.1257/jep.32.4.201

Hansen, M., Köhntopp, K., & Pfitzmann, A. (2002). The Open Source approach—Opportunities and limitations with respect to security and privacy**This paper was presented at ISSE 2001, September 26–28, London. This version is slightly revised. *Computers & Security, 21*(5), 461-471. https://doi.org/10.1016/S0167-4048(02)00516-3

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2022). *Probably Something : A Multi-Layer Taxonomy of Non-Fungible Tokens* (arXiv:2209.05456). arXiv. https://doi.org/10.48550/arXiv.2209.05456

Heeks, R. (2002). Information Systems and Developing Countries : Failure, Success, and Local Improvisations. *The Information Society, 18*(2), 101-112. https://doi.org/10.1080/01972240290075039

Heeks, R. (2003). Most eGovernment-for-Development Projects Fail : How Can Risks be Reduced? *iGovernment Working Paper No. 14*. https://doi.org/10.2139/ssrn.3540052

Henfridsson, O., & Bygstad, B. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. *MIS Quarterly, 37*(3), 907-931.

Hoepman, J.-H., & Jacobs, B. (2007). Increased security through open source. *Communications of the ACM, 50*(1), 79-83. https://doi.org/10.1145/1188913.1188921

Hooda, A., Gupta, P., Jeyaraj, A., Giannakis, M., & Dwivedi, Y. K. (2022). The effects of trust on behavioral intention and use behavior within e-government contexts. *International Journal of Information Management, 67*, 102553. https://doi.org/10.1016/j.ijinfomgt.2022.102553

Huang, P., Guo, L., Li, M., & Fang, Y. (2019). Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare. *IEEE Internet of Things Journal*, *6*(5), 9200-9210. https://doi.org/10.1109/JIOT.2019.2929087

Husz, O. (2018). Bank Identity : Banks, ID Cards, and the Emergence of a Financial Identification Society in Sweden. *Enterprise & Society*, *19*(2), 391-429. https://doi.org/10.1017/eso.2017.43

Hutchings, A., & Jorna, P. (2015). *Misuse of information and communications technology within the public sector*.

ID4D. (2019). *Identity Authentication and Verification Fees Overview of Current Practices*. https://documents1.worldbank.org/curated/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf

ID4D. (2022). *Principles on Identification for Sustainable Development : Toward the Digital Age* [Text/HTML]. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age

IDEMIA. (2020). *Public Private Partnerships—Identity Management—Idemia*. https://www.idemia.com/wp-content/uploads/2021/02/public-private-partnerships-identity-management-idemia-brochure-202005.pdf

IGOD. (2023). *Integrated Government Online Directory*. https://igod.gov.in/organization/RM4zv3QBGZk0jujBKgGW

Iivari, J. (2007). A paradigmatic analysis of information systems as a design science. *Scandinavian Journal of Information Systems*, *19*(2), 39-64.

Immelt, J. R., Govindarajan, V., & Timble, C. (2009). *How GE Is Disrupting Itself*. https://hbr.org/2009/10/how-ge-is-disrupting-itself

International Center for Humanitarian Affairs. (2021). *DIGID Lessons Learnt from Kenya*. https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

Inuwa, I., Ononiwu, C., Kah, M. M. O., & Quaye, A. K. M. (2019). Mechanisms Fostering the Misuse of Information Systems for Corrupt Practices in the Nigerian Public Sector. In P. Nielsen & H. C. Kimaro (Éds.), *Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D* (Vol. 552, p. 122-134). Springer International Publishing. https://doi.org/10.1007/978-3-030-19115-3_11

ITU. (2014). *Establishing conformity and interoperability regimes : Basic guidelines*. https://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/CI_BasicGuidelines_February2014_E.pdf

ITU. (2023). *Digital-Public-Infrastructure-Brochure.pdf*. https://www.itu.int/initiatives/sdgdigital/wp-content/uploads/sites/2/2023/09/Digital-Public-Infrastructure-Brochure.pdf

ITU. (2018). *Digital Identity Roadmap Guide*. ITU. https://www.itu.int:443/en/publications/ITU-D/Pages/publications.aspx

Janowski, T. (2015). Digital government evolution : From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221-236. https://doi.org/10.1016/j.giq.2015.07.001

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle : Policy-makers be prepared! *Government Information Quarterly, 35*(4, Supplement), S99-S105. https://doi.org/10.1016/j.giq.2015.11.009

Kallela, J. (2008). *Federated Identity Management Solutions*.

Khera, R. (2017). Impact of Aadhaar on Welfare Programmes. *Economic and Political Weekly*, *52*(50), 61-70.

Klitgaard, R. (2011). Designing and Implementing a Technology-Driven Public-Private Partnership (Innovations Case Discussion : India's Project Aadhaar). *Innovations: Technology, Governance, Globalization, 6*(2), 67-72. https://doi.org/10.1162/INOV_a_00070

Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. *Philosophy & Technology, 35*(1), 8. https://doi.org/10.1007/s13347-022-00503-9

Koppenjan, J., & Groenewegen, J. (2005). Institutional design for complex technological systems. *International Journal of Technology, Policy and Management, 5*. https://doi.org/10.1504/IJTPM.2005.008406

Kröger, J. L., Miceli, M., & Müller, F. (2021). How Data Can Be Used Against People : A Classification of Personal Data Misuses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3887097

Kubicek, H., & Noack, T. (2010a). Different countries-different paths. Extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society, 3*. https://doi.org/10.1007/s12394-010-0063-x

Kubicek, H., & Noack, T. (2010b). The path dependency of national electronic identities. *Identity in the Information Society, 3*. https://doi.org/10.1007/s12394-010-0050-2

Kumar, R. L. (2004). A Framework for Assessing the Business Value of Information Technology Infrastructures. *Journal of Management Information Systems*, *21*(2), 11‑32. https://doi.org/10.1080/07421222.2004.11045801

Kundisch, D., Muntermann, J., Oberländer, A. M., Rau, D., Röglinger, M., Schoormann, T., & Szopinski, D. (2022). An Update for Taxonomy Designers : Methodological Guidance from Information Systems Research. *Business & Information Systems Engineering*, *64*(4), 421‑439. https://doi.org/10.1007/s12599-021-00723-x

Lacity, M., & Carmel, E. (2022). Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet. *MIS Quarterly Executive*, 241‑251. https://doi.org/10.17705/2msqe.00068

Lai, X., & Patrick Rau, P.-L. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, *124*, 106894. https://doi.org/10.1016/j.chb.2021.106894

Lanitis, A. (2010). *A survey of the effects of aging on biometric identity verification | International Journal of Biometrics*. https://dl.acm.org/doi/10.1504/IJBM.2010.030415

Leiteritz, R. J. (2001). Sovereignty, developing countries and international financial institutions : A Reply to David Williams. *Review of International Studies*, *27*(03). https://doi.org/10.1017/S0260210501004351

Leung, D., Nolens, B., Arner, D. W., & Frost, J. (2022). *Corporate Digital Identity : No Silver Bullet, but a Silver Lining* (SSRN Scholarly Paper 4505160). https://doi.org/10.2139/ssrn.4505160

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39‑71. https://doi.org/10.1016/j.jsis.2008.01.001

Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T., & Draheim, D. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership : Learning from the Case of Estonia. *Information Systems Frontiers*, *25*(6), 2439-2456. https://doi.org/10.1007/s10796-022-10363-5

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact : Proposing a bold research agenda. *European Journal of Information Systems*, *26*(6), 546-563. https://doi.org/10.1057/s41303-017-0066-x

Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020). Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 71-78. https://doi.org/10.1109/BRAINS49436.2020.9223292

Madon, S. (2015). ICT4D and e-Governance. In P. H. Ang & R. Mansell (Éds.), *The International Encyclopedia of Digital Communication and Society* (1re éd., p. 1-8). Wiley. https://doi.org/10.1002/9781118767771.wbiedcs114

Madon, S., Ranjini, C. R., & Anantha Krishnan, R. K. (2022). Aadhaar and social assistance programming : Local bureaucracies as critical intermediary. *Information Technology for Development*, *28*(4), 705-720. https://doi.org/10.1080/02681102.2021.2021130

Madon, S., & Schoemaker, E. (2021). Digital identity as a platform for improving refugee management. *Information Systems Journal*, *31*. https://doi.org/10.1111/isj.12353

Magwedere, M. R., & Marozva, G. (2023). Does political risk matter for infrastructure investments? Empirical evidence. *Development Studies Research*, *10*(1), 2146596. https://doi.org/10.1080/21665095.2022.2146596

Mankoff, J., Kasnitz, D., Studies, D., Camp, L. J., Lazar, J., & Hochheiser, H. (2022). *Areas of Strategic Visibility : Disability Bias in Biometrics*. https://doi.org/10.48550/ARXIV.2208.04712

Manny, L., Angst, M., Rieckermann, J., & Fischer, M. (2022). Socio-technical networks of infrastructure management : Network concepts and motifs for studying digitalization, decentralization, and integrated management. *Journal of Environmental Management*, *318*, 115596. https://doi.org/10.1016/j.jenvman.2022.115596

Manurung, H. (2021). Myanmar Political Instability : A Threat to Southeast Asia Stability. *Jurnal Asia Pacific Studies*, *5*. https://doi.org/10.33541/japs.v5i1.2671

Markard, J. (2009). *Characteristics of Infrastructure Sectors and Implications for Innovation Processes*. https://www.semanticscholar.org/paper/Characteristics-of-Infrastructure-Sectors-and-for-Markard/10e36720017ffaf0c0daa0a76ef0d46202e4bcfa

Martin, A., & Taylor, L. (2021). Exclusion and inclusion in identification : Regulation, displacement and data justice. *Information Technology for Development*, *27*(1), 50-66. https://doi.org/10.1080/02681102.2020.1811943

Masiero, S. (2018). Explaining trust in large biometric infrastructures : A critical realist case study of India’s Aadhaar project. *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, *84*(6), e12053. https://doi.org/10.1002/isd2.12053

Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society*, *10*(1), 20539517221135176. https://doi.org/10.1177/20539517221135176

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, *31*(6), 903-928. https://doi.org/10.1111/isj.12351

Mathrani, A., Sarvesh, T., & Umer, R. (2022). Digital divide framework : Online learning in developing countries during the COVID-19 lockdown. *Globalisation, Societies and Education*, *20*(5), 625-640. https://doi.org/10.1080/14767724.2021.1981253

Mavroudis, V., Hicks, C., & Crowcroft, J. (2021). An Interface Between Legacy and Modern Mobile Devices for Digital Identity. In A. Saracino & P. Mori (Éds.), *Emerging Technologies for Authorization and Authentication* (p. 68-76). Springer International Publishing. https://doi.org/10.1007/978-3-030-93747-8_5

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII)* (NIST SP 800-122; 0 éd., p. NIST SP 800-122). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122

McKinsey. (2019). *Digital identification : A key to inclusive growth*.

Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of power inscription into governance : Lessons from two national digital identity systems. *Information Systems Journal*, *32*(2), 242-277. https://doi.org/10.1111/isj.12325

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation : Results from expert interviews. *Government Information Quarterly*, *36*(4). Scopus. https://doi.org/10.1016/j.giq.2019.06.002

Milner, H. V., Nielson, D. L., & Findley, M. G. (2016). Citizen preferences and public goods : Comparing preferences for foreign aid and government programs in Uganda.

The Review of International Organizations, *11*(2), 219-245. https://doi.org/10.1007/s11558-016-9243-2

Ministry of Electronics and IT. (2023). *MeitY proposes rules to enable Aadhaar authentication by entities other than Government Ministries and Departments*. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1918183

Ministry of Justice, India. (2019). *The Aadhaar and other laws (amendment) Act 2019*. https://uidai.gov.in/images/news/Amendment_Act_2019.pdf

Mir, U. B., Kar, A. K., Gupta, M. P., & Sharma, R. S. (2019). Prioritizing Digital Identity Goals – The Case Study of Aadhaar in India. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, & M. Mäntymäki (Éds.), *Digital Transformation for a Sustainable Society in the 21st Century* (Vol. 11701, p. 489-501). Springer International Publishing. https://doi.org/10.1007/978-3-030-29374-1_40

Mittal, A. (2022). *Catalog of Technical Standards for Digital Identification Systems*. https://documents1.worldbank.org/curated/en/707151536126464867/pdf/Catalog-of-Technical-Standards-for-Digital-Identification-Systems.pdf

Mosero, R. (2021). Analysing the impact of Digital ID frameworks on Marginalised Groups in Sub-Saharan Africa. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3797506

National Audit Office. (2019). *Investigation into Verify (Summary)*.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*, 336-359. https://doi.org/10.1057/ejis.2012.26

NIMC. (2022). *Data Privacy via Tokenization*. Nigeria Data Privacy Initiative. https://wiki.nimc.gov.ng/en/privacy/data-protection/tokenization

NIPFP. (2012). *A cost-benefit analysis of Aadhaar—National Institute of Public Finance and Policy*. https://macrofinance.nipfp.org.in/FILES/uid_cba_paper.pdf

NITI Aayog. (2020). *Blockchain : The India Strategy Part I*. https://www.niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

Nyst, C., Pannifer, S., Whitley, E. A., & Makin, P. (2016, juin 8). *Digital identity : Issue analysis* [Monograph]. Consult Hyperion. http://www.chyp.com/

OECD. (2023). *Recommendation of the Council on the Governance of Digital Identity*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

Okunoye, B. (2022). Mistrust of government within authoritarian states hindering user acceptance and adoption of digital IDs in Africa : The Nigerian context. *Data & Policy*, *4*. https://doi.org/10.1017/dap.2022.29

Our World In Data. (2023). *Income inequality vs. GDP per capita*. Our World in Data. https://ourworldindata.org/grapher/gini-coefficient-vs-gdp-per-capita-pip?xScale=linear&time=2020

Pali, I., Krishania, L., Chadha, D., Kandar, A., Varshney, G., & Shukla, S. (2020). *A Comprehensive Survey of Aadhar and Security Issues* (arXiv:2007.09409). arXiv. https://doi.org/10.48550/arXiv.2007.09409

Park, S., & Humphry, J. (2019). Exclusion by design : Intersections of social, digital and data exclusion. *Information, Communication & Society*, *22*(7), 934-953. https://doi.org/10.1080/1369118X.2019.1606266

Parliament of Bhutan. (2023). *National_Digital_Identity_Act_of_Bhutan_2023F.pdf*. https://www.nab.gov.bt/assets/uploads/docs/acts/2023/National_Digital_Identity_Act_of_Bhutan_2023F.pdf

Perez, S., Cabrera, J., Rodriguez, J., & Raymundo, C. (2019). *E-Government Adoption Model Extended with Public Value in Peru*. 338-342. Scopus. https://doi.org/10.1109/ICITM.2019.8710646

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293-310. https://doi.org/10.1177/1461444816661553

Présidence de la République de Guinée. (2022). *Decret D-2022-0134 portant création, attributions et fonctionnement de l'ONECI*.

President's Secretariat. (1979). *Rank and Precedence of Indian officials*. https://www.mha.gov.in/sites/default/files/table_of_precedence.pdf

Press Information Bureau. (2017). *UIDAI demonstrate at Zero Tolerance against unauthorized Agencies and Websites*. https://pib.gov.in/newsite/PrintRelease.aspx?relid=157985

Press Information Bureau. (2023). *UIDAI's relentless initiatives lead to strengthening of Aadhaar eco-system*. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1909255

Prichard, E. C. (2021). Is the Use of Personality Based Psychometrics by Cambridge Analytical Psychological Science's "Nuclear Bomb" Moment? *Frontiers in Psychology*, *12*, 581448. https://doi.org/10.3389/fpsyg.2021.581448

PwC. (2021). *PwC-Studie : Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche*.

Radiya-Dixit, E., & Neff, G. (2023). A Sociotechnical Audit : Assessing Police Use of Facial Recognition. *2023 ACM Conference on Fairness, Accountability, and Transparency*, 1334-1346. https://doi.org/10.1145/3593013.3594084

Reuben, W., & Carbonari, F. (2017). Identification as a National Priority : The Unique Case of Peru. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3013395

Robertson, V. H. S. E. (2019). *Excessive Data Collection : Privacy Considerations and Abuse of Dominance in the Era of Big Data* (SSRN Scholarly Paper 3408971). https://doi.org/10.2139/ssrn.3408971

Rocha, J. (2020). Spanish and portuguese eIDAS node evolution for electronic identification of European citizens. *Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, 1‑5. https://doi.org/10.1145/3401895.3402094

Ross, A., Banerjee, S., & Chowdhury, A. (2022). Deducing health cues from biometric data. *Computer Vision and Image Understanding*, *221*, 103438. https://doi.org/10.1016/j.cviu.2022.103438

Sallam, M., Lips, S., & Draheim, D. (2022). *Success and Success Factors of the Estonian E-Residency from the State and Entrepreneur Perspective* (p. 291‑304). https://doi.org/10.1007/978-3-031-04238-6_22

Sarkar, S. (2014). The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India. *Oxford Development Studies*, *42*(4), 516‑533. https://doi.org/10.1080/13600818.2014.924493

Sarkis, J., Koo, C., & Watson, R. T. (2013). Green information systems & technologies – this generation and beyond : Introduction to the special issue. *Information Systems Frontiers*, *15*(5), 695‑704. https://doi.org/10.1007/s10796-013-9454-5

Saunders, C., Benlian, A., Henfridsson, O., & Wiener, M. (2020, novembre 23). *IS Control & Governance*. MIS Quarterly. https://www.misqresearchcurations.org/blog/2020/11/23/is-control-amp-governance

Schelenz, L., & Pawelec, M. (2021). Information and Communication Technologies for Development (ICT4D) critique. *Information Technology for Development*, *28*(1), 165-188. https://doi.org/10.1080/02681102.2021.1937473

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2021). Identity at the margins : Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development*, *27*(1), 13-36. https://doi.org/10.1080/02681102.2020.1785826

Schoemaker, E., Martin, A., & Weitzberg, K. (2023). Digital Identity and Inclusion : Tracing Technological Transitions. *Georgetown Journal of International Affairs*, *24*(1), 36-45. https://doi.org/10.1353/gia.2023.a897699

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*, 1-16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Schwalm, S., & Alamillo-Domingo, I. (2022). *Self-Sovereign-Identity & eIDAS : A Contradiction? Challenges and Chances of eIDAS 2.0**. 89-108. https://doi.org/10.53136/979125994752910

Secure Identity Alliance. (2019). *Putting government back in control—Solving vendor lock-in with open standards*. https://www.id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology : Beyond Myth. *Business & Information Systems Engineering*, *62*(6), 599-608.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, *63*, 603-613. https://doi.org/10.1007/s12599-021-00722-y

Seidel, S., Bharati, P., Fridgen, G., Watson, R., Albizri, A., Boudreau, M.-C., Butler, T., Chandra Kruse, L., Guzman, I., Karsten, H., Lee, H., Melville, N., Rush, D., Toland, J., & Watts, S. (2017). The Sustainability Imperative in Information Systems Research. *Communications of the Association for Information Systems*, *40*. https://doi.org/10.17705/1CAIS.04003

Sharma, H., & Díaz Andrade, A. (2023). Digital financial services and human development : Current landscape and research prospects. *Information Technology for Development*, *29*(4), 582-606. https://doi.org/10.1080/02681102.2023.2199189

Shirlow, P. (2021). Lustration in Iraq : Regime change as exclusion and control. *Capital & Class*, *45*(1), 123-144. https://doi.org/10.1177/0309816820924400

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management : The Implications to Personal Data Protection. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 30-35. https://doi.org/10.1109/AINS47559.2019.8968708

Sporny, M., Longely, D., & Chadwick, D. (2019). *Verifiable Credentials Data Model 1.0*. W3C Recommendation.

Sridhar, S., Altinkemer, K., & Rees, J. (2005). *Software Vulnerabilities : Open Source versus Proprietary Software Security*.

Swiss Federal Counsel. (2021). *Arrêté du Conseil fédéral constatant le résultat de la votation populaire du 7 mars 2021*. https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2021/1185/de/pdf-a/fedlex-data-admin-ch-eli-fga-2021-1185-de-pdf-a.pdf

Swiss Federal Counsel. (2023). *E-ID : adoption du message par le Conseil fédéral*. https://www.bj.admin.ch/bj/fr/home/aktuell/mm.msg-id-98758.html

Tavares, A. P., & Masiero, S. (2023). *Digital Identity and Social Protection Programs : Leaving No One Behind?*

Taylor, J. A., Lips, M., & Organ, J. (2008). Identification practices in government : Citizen surveillance and the quest for public service improvement. *Identity in the Information Society*, *1*(1), 135. https://doi.org/10.1007/s12394-009-0007-5

Temoshok, D., Richer, J., Choong, Y.-Y., Fenton, J., Lefkovitz, N., & Regenscheid, A. (2022). *Digital Identity Guidelines : Federation and Assertions* (NIST Special Publication (SP) 800-63C-4 (Draft)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63C-4.ipd

The Alan Turing Institute. (2021). *Openness in the digital identity context*. The Alan Turing Institute. https://www.turing.ac.uk/programme/openness-digital-identity-context

Thoburn, M. (2012). *Identification, Surveillance and Profiling : On the Use and Abuse of Citizen Data—Seeking Security*. http://www.bloomsburycollections.com/collections/monograph-detail

Thomas, S. (1998). User fees, self-selection and the poor in Bangladesh. *Health Policy and Planning*, *13*(1), 50-58. https://doi.org/10.1093/heapol/13.1.50

Tiwari, K., & Gupta, P. (2014). Fingerprint Quality of Rural Population and Impact of Multiple Scanners on Recognition. In Z. Sun, S. Shan, H. Sang, J. Zhou, Y. Wang, & W. Yuan (Éds.), *Biometric Recognition* (p. 199-207). Springer International Publishing. https://doi.org/10.1007/978-3-319-12484-1_22

Aadhaar policy on pricing, (2020). https://uidai.gov.in/images/akr_policy_on_pricing.pdf

UIDAI. (2022a). *UIDAI_Annual_Report_21_22.pdf*. https://uidai.gov.in/images/UIDAI_Annual_Report_21_22.pdf

UIDAI. (2010). *UIDAI STRATEGY OVERVIEW*. https://prsindia.org/files/bills_acts/bills_parliament/2010/UIDAI_STRATEGY_OVERVIEW.pdf

UIDAI. (2018). *Enhancing Privacy of Aadhaar holders—Implementation of Virtual ID, UID Token and Limited KYC*. https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf

UIDAI. (2019a). *NRI Aadhaar Enrolment*. https://uidai.gov.in/images/resource/NRI_Aadhaar_Enrolment_23092019.pdf

UIDAI. (2019b). *What is Aadhaar KYC? Know e-KYC for Aadhaar card*. https://uidai.gov.in/images/news/What-is-Aadhaar-KYC-Know-e-KYC-for-Aadhaar-card.pdf

UIDAI. (2022b). *Clarifications on issues relating to sharing of Aadhaar and related data amongst government departments*. https://uidai.gov.in/images/UIDAI_OM_dated_15.07.2022.pdf

UIDAI. (2022c). *Training, Testing & Certification Ecosystem*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/ecosystem/training-testing-certification-ecosystem.html

UIDAI. (2023a). *Aadhaar Paperless Offline e-kyc*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/contact-support/have-any-question/307-faqs/aadhaar-online-services/aadhaar-paperless-offline-e-kyc.html

UIDAI. (2023b). *Authentication*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/contact-support/have-any-question/303-english-uk/faqs/authentication.html

UIDAI. (2023c). *Enrolment Agencies*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/ecosystem/enrolment-ecosystem/enrolment-agencies.html

UIDAI. (2023d). *Finance & Accounts*. Unique Identification Authority of India | Government of India. https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india/finance-accounts.html

UN LIEG. (2019). *United Nations Strategy for Legal Identity for All*. https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf

UNCDF. (2020). *RFA Feasibility Study for setting up a single identification system for financial service users in the WAEMU (UEMOA)*.

UNDP. (2023). *Undp-the-dpi-approach-a-playbook.pdf*. https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-the-dpi-approach-a-playbook.pdf

UNHCR. (2018). *UNHCR Strategy on Digital Identity and Inclusion*.

USAID. (2017). *Identity in a Digital Age : Infrastructure for Inclusive Development*. https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, *22*(5), 896-914. https://doi.org/10.1177/1461444819872537

Varma, P. (2010). *Aadhaar Scalability & Data Management Challenges*. https://www.cse.iitb.ac.in/~comad/2010/pdf/Industry%20Sessions/UID_Pramod_Varma.pdf

Verheul, E., & Jacobs, B. (2017). *Polymorphic encryption and pseudonymisation in identity management and medical research*.

Veseli, F., Olvera, J. S., Pulls, T., & Rannenberg, K. (2019). Engineering privacy by design : Lessons from the design and implementation of an identity wallet platform. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 1475-1483. https://doi.org/10.1145/3297280.3297429

W3C. (2022a). *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core/

W3C. (2022b). *Verifiable Credentials Data Model v1.1*. https://www.w3.org/TR/vc-data-model/

Wachter, S., & Mittelstadt, B. (2018). *A Right to Reasonable Inferences : Re-Thinking Data Protection Law in the Age of Big Data and AI* (SSRN Scholarly Paper 3248829). https://papers.ssrn.com/abstract=3248829

Walke, F., Winkler, T., & Le, M. (2023). *Success of Digital Identity Infrastructure : A Grounded Model of eID Evolution Success*.

Wang, F., & Filippi, P. (2020). Self-Sovereign Identity in a Globalized World : Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, 28. https://doi.org/10.3389/fbloc.2019.00028

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets*, *12*(3), 157-162. https://doi.org/10.1080/101967802320245929

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2022). The EU’s Digital Identity Policy : Tracing Policy Punctuations. *15th International Conference on Theory and Practice of Electronic Governance*, 74-81. https://doi.org/10.1145/3560107.3560121

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of Self-Sovereign Identity : An Extended Model of Interpretive Flexibility. *Proceedings of the Hawaii International Conference on System Sciences 2022*, 2543-2552.

Weitzberg, K., Cheesman, M., Martin, A., & Schoemaker, E. (2021). Between surveillance and recognition : Rethinking digital identity in aid. *Big Data & Society*, *8*(1), 20539517211006744. https://doi.org/10.1177/20539517211006744

Welch, E. W., Hinnant, C. C., & Jae, M. M. (2004). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory*, *15*(3), 371‑391. https://doi.org/10.1093/jopart/mui021

Wickins, J. (2007). The ethics of biometrics : The risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics*, *13*(1), 45‑54. https://doi.org/10.1007/s11948-007-9003-z

Williams, D. (2000). Aid and sovereignty : Quasi-states and the international financial institutions. *Review of International Studies*, *26*(4), 557‑573. https://doi.org/10.1017/S026021050000557X

Wimmer, M. A., Pereira, G. V., Ronzhyn, A., & Spitzer, V. (2020). Transforming government by leveraging disruptive technologies : Identification of research and training needs. *eJournal of eDemocracy and Open Government*, *12*(1), 87‑114. Scopus. https://doi.org/10.29379/jedem.v12i1.594

Witten, B., Landwehr, C., & Caloyannides, M. (2001). Does open source improve system security? *IEEE Software*, *18*(5), 57‑61. https://doi.org/10.1109/52.951496

Woo, J., & Kumar, M. S. (2015). Public Debt and Growth. *Economica*, *82*(328), 705‑739. https://doi.org/10.1111/ecca.12138

World Bank. (2014). *Digital Identity Toolkit*. https://openknowledge.worldbank.org/server/api/core/bitstreams/ec566c87-09c4-5171-ab8d-9f3707c613f0/content

World Bank. (2018). *International Development Association project appraisal document on a proposed credits and grant to the republic of Côte d'Ivoire & the*

Republic of Guinea. https://documents1.worldbank.org/curated/en/771571528428669934/pdf/REGIONAL-INTEGRATION-CAS-AFRICArev-05152018.pdf

World Bank. (2021a). *ID4D GLOBAL DATASET - Volume 1 2021 : Global ID Coverage Estimates* [Text/HTML]. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099705012232226786/P176341032c1ef0b20adf10abad304425ef

World Bank. (2022a). *Federated Ecosystems for Digital ID : Current Approaches and Lessons*. World Bank. https://doi.org/10.1596/38443

World Bank. (2023a). *The West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program : Unique Identifiers to Enable Access to Human Development Services*. Washington, DC: World Bank. https://doi.org/10.1596/40121

World Bank. (2019a). *ID4D Practitioner's Guide.pdf.* https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

World Bank. (2019b). *Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable*. World Bank. https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

World Bank. (2019c). *Procurement-Guide-And-Checklist-For-Digital-Identification-Systems.pdf.* https://documents1.worldbank.org/curated/en/104171583178428889/pdf/Procurement-Guide-And-Checklist-For-Digital-Identification-Systems.pdf

World Bank. (2021b). *The Global Findex 2021 : Interactive Executive Summary Visualization* [Text/HTML]. World Bank. https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization

World Bank. (2022b). *Identification for Development (ID4D) and Digitalizing G2P Payments (G2Px) 2022 Annual Report* [Text/HTML]. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099437402012317995/IDU00fd54093061a70475b0a3b50dd7e6cdfe147

World Bank. (2023b). *Creating Digital Public Infrastructure for Empowerment, Inclusion, and Resilience*. World Bank. https://projects.worldbank.org/en/results/2023/10/12/creating-digital-public-infrastructure-for-empowerment-inclusion-and-resilience

Zdjelar, R., & Žajdela Hrustek, N. (2021). Digital Divide and E-Inclusion as Challenges of the Information Society – Research Review. *Journal of Information and Organizational Sciences, 45*(2), 601-638. https://doi.org/10.31341/jios.45.2.14

The EU's Digital Identity Policy: Tracing Policy Punctuations

Linda Weigl*
University of Luxembourg, Luxembourg

Alexandre Amard*
University of Luxembourg, Luxembourg

Cristiano Codagnone
University of Milan, Italy

Gilbert Fridgen
University of Luxembourg, Luxembourg

ABSTRACT

This paper analyzes the development of the European Union's digital identity policy. The analysis focuses on the dynamics leading to a sudden shift from identity management as a sensitive topic under national competence towards a common, harmonized, user-centric European Digital Identity Framework layering on top of Member States' existing systems. We adopted a syncretic approach to Punctuated Equilibrium Theory and focused specifically on the concept of policy punctuations and policy image. Process tracing is used as a method to trace and interpret causal mechanisms of policy processes. The empirical analysis is grounded in elite interviews and policy documentation. To open up the black box of policy-making, we analyze and disaggregate the policy process. We thereby provide a better understanding of the historical-political and technological mechanisms that determine particular policy outcomes.

CCS CONCEPTS

• **Social and professional topics**; • **Computing / technology policy**; • **Government technology policy**; • **Governmental regulations**;

KEYWORDS

eIDAS, European Digital Identity Framework, Digital identity, Punctuated equilibrium theory, Process tracing, Policy process

ACM Reference Format:
Linda Weigl, Alexandre Amard, Cristiano Codagnone, and Gilbert Fridgen. 2022. The EU's Digital Identity Policy: Tracing Policy Punctuations. In *15th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2022), October 04–07, 2022, Guimarães, Portugal.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3560107.3560121

1 INTRODUCTION

With rising concerns about citizens and businesses losing control over their data [22, 36], governments, and the European Union (EU) in particular, are engaging in the production of policies that regulate the digital sphere. A significant element of this 'cybernetic' [16] strategy is a pan-European digital identity management system [12]. The European Commission's[1] legislative proposal introducing such system emerged as the result of a revision in June 2021.

As such, the European Digital Identity Proposal [12][2] builds on the 2014 electronic Identification, Authentication and trust Services (eIDAS) Regulation[3]. The Proposal follows extensive reviewing and consultation efforts on the eIDAS Regulation. The eIDAS review was anchored in Article 49 and thus determined to happen by law. However, prior to the start of the review, there were no officially announced plans to introduce a European Digital Identity scheme. Under the eIDAS Regulation, some Member States had already invested in their own electronic identification (eID) schemes [9]. Moreover, in the realm of identity management where identification is based on official electronic documents, the Treaty (TFEU) does not explicitly foresee regulatory competence for the EU to intervene in national affairs[4]. Plans to complement eIDAS with a European digital identity were first appearing on the legislative agenda in 2020. A Commission Communication of February 2020 [10] listed the 'review' of eIDAS as a 'revision'. In the Commission's Inception Impact Assessment, the European digital identity was introduced as one out of three 'policy options' to "strengthen Europe's technological autonomy [...] to compete globally" [15]. The speedy introduction of a proposal for a European Digital Identity Framework (EDIF), in a policy area where the EU's legal competence has been subject to interpretation, presents an interesting case of policy punctuation in the digital sphere. This gave rise to the following research question: *Why did a sudden step change occur in EU digital identity policy in the form of a substantial eIDAS revision?*

The importance of studying this phase of the policy process, the stage of '*agenda-setting*', lies in its function within the so-called '*policy cycle*' [21]. As the agenda-setting process defines which issues come to the fore in the first place, it determines to a large extent the chronology of events in subsequent phases. In light of the new EU digital constitutionalism and its increasingly complex legal construction [5, 7, 13], the necessity to thoroughly understand the process of a policy issue prior to its appearance on the political agenda becomes evident.

To answer our research question, we adopt a syncretic approach to theory. We study the policy development of the EDIF through

*Both authors contributed equally to this research.

[1] Hereinafter also referred to as 'Commission'.

[2] Proposal for amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

[3] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[4] Legal identities fall in the scope of Member States' competences, especially as it concerns their sovereignty to identify their own citizens. Nevertheless, the EDIF proposal's stated objectives are to enable a digital single market, protect consumers and to create a space of freedom, due to the potential abuses of gatekeeper platforms and companies, while maintaining security cross-border contexts; areas that are included within shared competences between the EU and Member States according to Article 4.2 (a), (f) and (j) TFEU.

ICEGOV 2022, October 04–07, 2022, Guimarães, Portugal
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9635-6/22/10.
https://doi.org/10.1145/3560107.3560121

the theoretical lens of Punctuated Equilibrium Theory (PET) to understand the process of sudden policy change in the EU. This process of change takes into account the shift from identity management as a sensitive policy area exclusively dealt with on the national stage, towards harmonization efforts within a European framework. We explain and disaggregate this policy process using the Process Tracing (PT) methodology. We thereby open up the black box of policy-making and provide a better understanding of mechanisms that determine policy outcomes.

2 BACKGROUND

2.1 The EU Digital Identity Policy

With a variety of services offered online in the last decades, new pathways for remote identity verification emerged [18, 37]. Given the impact of digitalization on the international environment, one characteristic of eID services is typically the transcendence of national borders. In the EU, the eIDAS Regulation of 2014 provides the basis for remote cross-border identification and thus plays a fundamental role in this regard [24, 32]. To enable cross-border recognition of eID, the eIDAS Regulation relies on voluntary, notified national eID schemes. For identification and authentication purposes, however, eIDAS is limited to public sector services, despite a majority of use cases lying with the private sector [32]. This restrains the EU's range of possibilities to provide an alternative to citizens for private authentication schemes enabling equally convenient mechanisms such as Single Sign-On.

The 2021 evaluation of eIDAS highlighted that it had been highly successful in achieving technical interoperability for trust services, but it criticized the limitation to public sector services and the lack of incentive for Member States and private identity providers to connect to the infrastructure. These shortcomings had led to a low uptake by citizens and Member States, which paved the way for opportunities of private parties to build, offer and control user-friendly eID solutions. This raises particular concerns about a decline in individuals' control over their personal data [36], as well as a decline in governments' digital sovereignty and controlling power more generally [16]. Floridi highlights this 'poietic power' of companies that governments depend on for a variety of issues in the digital sphere. In the EU's eID landscape, this innovation asymmetry between states and companies is evidenced by another shortcoming. Not all Member States run eID schemes, and even fewer have notified them to the Commission. On top of that, individual national standards lead to large discrepancies between countries' eID schemes' implementations [24]. Overall, this means that cross-border transactions are limited and many services are not accessible under eIDAS.

In a Communication entitled *2030 Digital Compass: the European way for the Digital Decade* [11] published in March 2021, the Commission presented an update of its digital strategy, including an envisioned uptake of eID systems by 80% of citizens by 2030. In June 2021, the Commission put forth a legislative proposal with binding legal force throughout the EU. The EDIF proposal introduces digital wallets which would enable citizens to verify their identity online to access both public and private services without having to resort to commercial providers. Moreover, the Commission's proposal is "extraterritorial", as Recital 28 and Article 12b on the cross-border reliance on European Digital Identity Wallets mandate very large online platforms, none of which being European, "to accept the use of European Digital Identity Wallets" for the provision of services where user authentication is required. It thereby exercises a de facto and de jure '*Brussels effect*' "with the consequence that market players must deal with EU regulations regardless of where they operate if such operations affect EU citizens" [7]. At the time of writing, this legislative proposal is awaiting the European Parliament's responsible Committee decision and will be transferred to the Council of the EU thereupon.

It may appear that - despite its high level of ambition to set out a harmonized legal framework across the EU - the development of the Proposal corresponds to a natural evolution of demands. Yet, in light of the dynamic evolution of this Proposal, this explanation might be oversimplified. The study of agenda-setting holds that there is a nearly unlimited amount of important policy issues and corresponding policy solutions that could rise to the top of the political agenda [4]. In reality, only a few policies will catch the limited attention spans of policy-makers [27], while the vast majority remains ignored. We thus look into agenda-setting theory to understand why the revision of the 2014 eIDAS Regulation was translated into a new legislative proposal for the EDIF in 2021.

2.2 Agenda-Setting in the European Union

We study the policy process of the EDIF through the theoretical lens of PET [1, 31]. PET is used to explain long periods of policy stability 'punctuated' by outbursts of policy activity resulting in major policy changes. In their seminal work *Agendas and Instability in American Politics*, Baumgartner and Jones elaborate on PET. In applying this framework to the European institutional set up, Princen [26, 27] refined some of the key concepts of PET.

The EU's policy on eID was stable throughout several years. This stability is reflected in the careful take on eID adopted by the eIDAS Regulation in 2014. This phase of stability marks a first period (P1, see Figure 1) in the EU's digital identity policy, starting with the legislative proposal for the eIDAS Regulation in 2012, and terminating with the end of the Juncker Commission in 2019. In contrast, the 2021 new legislative proposal is a striking and ambitious policy change. Under the Proposal, Member States are obliged to notify at least one eID scheme - a previously voluntary requirement. It further introduces obligations for specific private sector actors to accept the use of the proposed EU Digital Wallet. Based on legislative dynamics that oblige both public and private sector to engage substantial resources in an area where the EU's legal legitimacy was perceived to be limited, we argue that the EDIF proposal punctuates the equilibrium in the development of Europe's digital identity policy. We refer to this as the policy punctuation hypothesis (H_{pp}): *The introduction of a speedy and ambitious proposal on a European Digital Identity Framework is a clear step change in a previously stable European digital identity policy.*

Princen [26, 27] offers a detailed framework for policy change in the EU. He emphasizes '*policy venues*' and '*problem definition*', the latter consisting of the '*policy image*', or so-called '*frames*', as key concepts that oscillate between policy stability and change. The venue of a policy plays an important role as policy issues can be perceived differently by different audiences [4] and due to the fundamental difference between institutional arenas, such as the dynamics of participation, institutional authority, credibility,

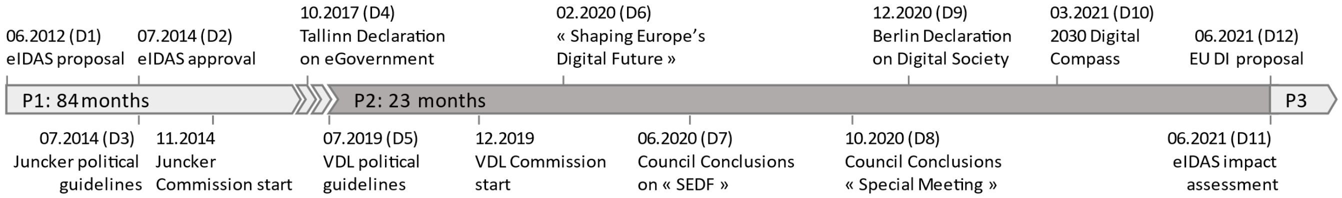


Figure 1: Timeline of key events, publications (see Appendix 2, Table 2) and periods in the policy-making process. VDL = European Commission President von der Leyen. SEDF = Communication on "Shaping Europe's Digital Future".

the support base for a certain policy, political priorities, general interests and networks [26]. Therefore, it is important to specify the venue in which a policy will be taken up. The intentional selection of a venue by policy-makers to influence policy outcomes is called '*venue-shopping*', a key element in the policy punctuation dynamic [1]. The issue itself remains unchanged, but the environment of policy actors varies according to the institutional space and scope of participation of the venue. Political actors can shift the discussion of a topic horizontally from one policy sector to another, or vertically e.g., from the national to the supranational level [27].

Next to institutional venues, Princen highlights the bounded rationality of policy actors who are subject to cognitive limitations which are predetermined and reinforced by institutional structures [27]. Decision- and policy-makers can only dedicate their attention to one issue at a time and each governmental unit is usually allocated to one specific task. Within this limited attention span, policy issues compete by being defined in a way that convinces the audience of its urgency and priority [1]. This can be achieved through the 'problem definition' or the 'frame' of a policy issue, "a mixture of empirical information and emotive appeals" that defines how it is portrayed and placed in a context to get the most attention from the audience in the political debate [31]. Attention for an issue can also be gained by utilizing already existing public attention and placing the issue in that context. This allows issue proponents to accentuate the importance and urgency of one policy issue, while minimizing the attention in the established reference for another.

In the EU's policy process on digital identity, a decisive event was the new Commission mandate under President von der Leyen, appointed in December 2019. This defines a second critical period (P2, see Figure 1) for our analysis. The Commission put forth the idea of a European digital identity for the first time publicly in a Communication entitled *Shaping Europe's Digital Future* [10]. The Communication maps out future plans for one of the six political priorities of European Commission President von der Leyen. Specifically, it calls for "helping consumers take greater control of - and responsibility for - their own data and identity" through a "universally accepted public electronic identity [...] without having to use unrelated platforms [...] and unnecessarily sharing personal data with them". The differentiation of "them", i.e., large, mostly non-EU technology companies, is becoming an increasingly important motive in the communication strategy of the EU digital policy-making process. This also aligns with the novel inception of digital constitutionalism which Celeste [5] explains as "constitutional counteractions against the challenges produced by digital technology". From this emerges the politically-embedded notions of *'digital sovereignty'* and *'strategic autonomy'* [6] as means of exercising controlling power and advancing the concept of European leadership in the global digital domain.

Importantly, actors across the entire political system shift policy attention collectively. As a result, such shifts are not the "province of one partisan camp alone" and cannot be accounted for and explained solely within "the confines of the standard model based in preference shifts caused by electoral change" [19]. Moreover, contrary to the agenda-setting perspective as a theory of policy dynamics, the comparative statics approach has "conflated the choice of policy issue (agenda setting) with the policy solution chosen given a policy problem" [19]. According to Jones and Baumgartner, political parties and partisan interests play a rather minor role at the problem stage. At the solution stage, on the other hand, ideology and partisanship are a far more relevant aspect to consider. From a problem perspective, the last decades witnessed rising power asymmetries between users and service providers [36] and a well-established digital corporate sovereignty built on the hegemonic positions of non-European multinational technology companies [16].

Considering the rising strategic importance of identity in the digital world, concerns are raised over the increasing power of these companies, their economic and social influence, and the threat they constitute to Europe's ability to act independently in this domain [22]. In response to these dynamics, the von der Leyen Commission identified a number of digital policy priorities that would sustain economic growth and strengthen the EU's global competitiveness. While the eIDAS Regulation aimed at facilitating digital cross-border administration, the proposed EDIF matured as a legislation to strengthen Europe's stance in the geopolitics of data. We posit that this shift in discourse signals a change in the policy image of eID: because the new policy image is linked to overarching political priorities of the Commission, the policy was able to expand to the macro-political level. This led to the June 2021 EDIF proposal, which marks the third and final period (P3, see Figure 1) of the policy process analyzed in this paper. We refer to this as the policy image hypothesis (H_{pi}): *The linking of the eIDAS Regulation with the European Commission's digital priorities punctuated the equilibrium of the European digital identity policy.* It focuses on the concept of policy image within PET, which allows us to highlight the role played by the framing of a policy within complex policy processes.

3 METHODOLOGY

3.1 Process Tracing

Process Tracing (PT) methodology is rooted in the logic of causal mechanisms for within-case accounts of policy change [2, 8]. Its objective is to move beyond the description of empirical narratives and instead identify causal mechanisms that link causes and outcomes to craft fine-grained explanations of policy change. In the field of policy studies, there have been increasing calls for analyzing causal mechanisms in policy-process theory [33]. Within many policy process theories, “causation is often claimed or implied, and at best supported by shallow explanations” [33]. Capturing causal mechanisms with PT methodology can strengthen the analysis of policy processes of single case studies by providing a robust method to understand causality. In practice, a nuanced understanding of policy-making disaggregates the policy process into cause-and-effect mechanisms between different factors, such as focusing events or policy-makers' attention to policy problems [2]. PT can be modelled as: X caused Y through a mechanistic process of *A*, *B*, *C* in case *Z* [20].

The typically theory-centric PT approach [2] requires the underlying theoretical model to be translated into a causal mechanism. In our case, each step in a sequence of policy development is explained by reference to PET. As a ‘theory of policy dynamics’ [19], PET seems to be a particularly well positioned theoretical foundation for unravelling causal mechanisms that lead to policy change. The mechanistic approach is central to PET, as episodic policy changes are triggered by, for instance, focusing events or changing actor constellations. In an introduction to a special issue on PET, Jones and Baumgartner [19] called for empirical in-depth analyses of policy processes in which “causes of punctuated equilibrium could fruitfully be studied by interviews and process tracing using government documents”.

3.2 Data Collection and Data Analysis

The study builds on secondary evidence consisting of 10 semi-structured elite interviews and primary evidence drawn from policy documentation [30]. The interviews were conducted between March 2022 and April 2022, and lasted on average about 40 minutes. Only interviewees involved into the decision- and policy-making process were selected (see Appendix, Table 1). Their average professional experience is 25 years and 6 months. To triangulate our interview results, data has been gathered from 12 publicly accessible policy documents (see Appendix, Table 2). Using primary evidence allowed us to cross-check the causal inferences derived from our interview data. Two authors coded the interview transcripts and policy documentation using the qualitative analysis software MAXQDA [23]. Following our deductive theory-centric approach [2], we proceeded with closed coding using a pre-established coding scheme based on PET.

In order to test the two PET-derived hypotheses empirically, it is necessary to operationalize the variables in the causal mechanism of policy change. The eIDAS Regulation, published in 2014, constitutes the start of a period of policy stability and the status quo in the PET framework. Its policy image is expected to be a reflection of its functionalist purpose by enabling cross-border authentication and interoperability of Member States' systems in the EU. Consequentially, we operationalize this status quo with the key concepts ‘*cross-border*’ and ‘*interoperability*’. The EDIF is hypothesized to be a more political piece of legislation as it seeks to establish a more harmonized approach to digital identification, which is therefore argued to mark a punctuation in the policy equilibrium. ‘*Harmonization*’ is thus operationalized as a key concept to embody this major policy shift. To test H_{pi}, the identified digital policy priorities are (1) ‘*Digital sovereignty*’ (encompassing the independence from both foreign actors and powerful private sector actors), (2) ‘*Data control*’ (referring to the aspects of user-centricity related to data, including control, privacy and data protection), (3) ‘*Digital single market*’ (building a favorable environment for digital growth and better access to digital services), and (4) ‘*Competitiveness*’ (referring to the capacity to sustain a high rate of productivity growth) of the EU.

As highlighted above, we identified three key points in time for the testing of our hypotheses (See Figure 1). The first one is the period starting in 2012 with the legislative proposal for the eIDAS Regulation until 2019 (P1) which marks the end of the Juncker Commission. The second period, from July 2019 to June 2021 (P2), starts with the transition to the von der Leyen Commission, officially inaugurated in December 2019. The third period starts on the 3rd of June 2021 (P3), when the EDIF proposal was published. These 3 periods form our investigation space: P1 plotting our initial situation, P2 encompassing the stage in which causal processes took place, and P3 the outcome of the causal process.

4 FINDINGS

4.1 Policy Punctuation

PET focuses on major policy changes after longer periods of stability. With the eIDAS Regulation in 2014 (P1) it was “the first time [...] that different regulations at European level were brought together to create more consistency and [...] provide a consistent trust framework for the single market in the electronic area” (I7). This meant that the objectives of the eIDAS Regulation as a “federated solution” in 2014 were to provide a long-lasting legal basis for a European identity ecosystem and enable interoperable cross-border electronic authentication (I1, I3, I4, I5, I6, I8, D1, D2, D4).

The situation fundamentally changed since 2014, as the facilitation of cross-border access to online public services was no longer the central issue (I7). We thus hypothesized that the new legislative EDIF proposal in P3 marked a punctuation in the European digital identity policy equilibrium (H_{pp}). The analysis of our data collected from both interviews and policy documentation supported this. The proposed European Digital Identity policy option “presents the highest level of ambition” (I2, D12) and a “quantum leap” that will “forever change the framework on electronic and digital identities [...] to be a model for the rest of the world” (I9). In this context, the proposal was considered a “substantial change” and “complete paradigm shift [compared to] eIDAS 1.0, which was [...] humble or shy in its ambition [towards] a clear mandate to step up” (I2) and “harmonize the provision of eID at the EU level” (I1). Our data further demonstrated that the legislative proposal evolved beyond a pure review obligation as outlined in Article 49 of the eIDAS Regulation (I1). By increasingly gaining “urgency and importance” (I2, I3, I7, I9) backed up by "unusual" empowerment from the European Council (I9), the policy proposal "changed [the Commission's] entire mission related to the particular deliverable" (I1) in the course of P2. Drawing from the observed shift away from the legislation's functionalist purpose to regulate cross-border interactions and interoperability towards a harmonized digital identity ecosystem, we can confirm H_{pp} for the European Digital Identity proposal.

4.2 Policy Image

Digital sovereignty. In its Communication on Shaping Europe's Digital Future, published in February 2020, the Commission contextualized digital identity for the first time in the larger frame of "helping consumers take greater control of and responsibility for their own data and identity" by ensuring "clearer rules on the transparency, behavior and accountability of those who act as gatekeepers to information and data flows" (D6). It argued that "a universally accepted public electronic identity [...] is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them" (D6). In particular the "huge pressure" from large platforms (I2, I6) offering identification and authentication services to EU citizens for data exploitation purposes was confirmed as a large threat resulting in the importance and urgency for governments to act quickly and strategically (I1, I2, I3, I4, I6, I7, I8, D10). The Council Conclusions on *Shaping Europe's Digital Future*, published in June 2020, further acknowledged the power of large online platform companies as gatekeepers in the digital economy to draw vast amounts of data (D7). A clear need was stressed to establish limitations that would "prevent these big entities from scooping out the identity data that would be available in [digital] wallets" (I1, I7). This would "recover a little bit of the digital sovereignty that [the EU] had lost to these American platforms" (I6, I7, I8, D9). The purpose of digital sovereignty, in this context, was "to reduce [the EU's] dependency on other parts of the globe for most crucial technologies" (D6). This includes the objective "to make citizen and companies [...] regain their freedom to manage [...] data in the digital [world]" (I3). With "the realization that the power of the gatekeepers is just incommensurable" (I3), the eIDAS Regulation's raison d'être assimilated the legal objectives of the Digital Services Act and the Digital Market Act (I3, D12). The Impact Assessment accompanying the European Digital Identity proposal substantiated this by affirming that "technological sovereignty would [...] be enhanced through greater harmonization of the implementation of eIDAS" which "would [...] allow EU digital industry compete at equal footing with large online platforms in the provision of digital identity solutions" (D11).

Data control. Like digital sovereignty, data control figured prominently in all policy documents linked to the European digital identity. In February 2020, the Commission stressed that "people should also be able to control their online identity, when authentication is needed to access certain online services" (D6). In its conclusions on shaping Europe's digital future four months later, the Council of the EU not only stressed that EU citizens and businesses should retain control over their data, but also called "upon the Commission to [...] create a [...] framework for digital identity, safeguarding the competitive edge of European businesses and protecting the EU common values and fundamental rights, such as the protection of personal data and privacy" (D7). Likewise, in October 2020, the European Council highlighted the importance of an EU-wide digital identity framework "to provide people with control over their online identity and data" and invited "the Commission to come forward with a proposal for a 'European Digital Identification' initiative by mid-2021" (D8). This was identified as a clear, unanimous "mandate from the Member States" to "come up with a new proposal on a European Digital Identity Framework" (I2, I7). In the Berlin Declaration on *Digital Society and Value-Based Digital Government* from December 2020, the Presidency of the Council expressed its commitment to "continue working towards developing an EU-wide Digital Identity framework allowing citizens and businesses to [...] access online public and private services, while minimizing disclosure and retaining full control of data" (D9). The Digital Compass published in March 2021 (D10), the Impact Assessment report (D11), the Proposal itself (D12), and interview participants (I2, I3, I4, I6, I7, I8, I9) further highlighted the shift of the policy problem away from cross-border access to online public services towards providing a framework which ensures data control, protection and privacy.

Digital Single Market. In June 2020, the Council of the EU acknowledged that a European digital identity will be an "essential enabler of the digitalized Single Market" (D7), thereby linking the policy area of digital identity to the third key concept in the Commission's digital policy priorities. This was also reflected in some policy documents (D6, D9), in the Proposal itself (D12), and in an interview, where it was argued that the functioning of the Digital Single Market cannot "avoid fixing the aspect of identity" (I1). A comparison between Juncker's (D3) and von der Leyen's political priorities (D5) reveals that while data control took a rather minor and digital sovereignty a non-existent role in Juncker's political guidelines, the pursuit of a connected Digital Single Market to "make much better use of the great opportunities offered by digital technologies" and "break down national silos" loomed large.

Competitiveness. A similar pattern can be found in the fourth key concept. Competitiveness is a political objective in both the current and the previous Commission mandate (D3, D5). In comparison with the previously analyzed political priorities, our data provided less evidence for the policy image of the European digital identity to be embedded in this priority. Still, the Impact Assessment accompanying the European Digital Identity proposal maintained that the EDIF proposal would "boost global trade and support competitive advantage of the EU-based enterprises" and "foster the competitive advantage of European businesses globally, through greater digitalization [...] of their service offering" (D11). The European Digital Identity proposal reflects the same argumentation (D12).

4.3 Agenda-Setting Factors

Next to the political priorities of the Commission, our analysis yielded further insights into other agenda-setting factors at play. It was frequently argued that the "acceleration by the [Coronavirus Disease (COVID-19)] crisis" (I3, I4) enabled "digital identity and electronic signatures [to] show their usefulness [...] for the continuity of [...] fundamental services for society" (I1, I2). Policy documentation highlighted "the need for fast development of online public services that allow citizens to deal with public authorities remotely" (D7, D8, D12). Moreover, there was a certain ambiguity with regard to the impact of technological progress in the sphere of digital identity, specifically the Self-Sovereign Identity (SSI) movement. It was argued that clearly "[technological] developments since 2014 [such as the] concept of self-sovereign identities, [...] the wallet [and] verified attributes based on emerging [...] standards" caused a certain "political moment" (I1) and "inspiration" for the technical design (I10). Other interviewees maintained that "the push for [policy] has been [predominantly] the sanitary crisis" (I4), thereby imparting less importance to the role of "technological [breakthroughs]" in the agenda-setting process (I10). A third and final factor identified in our data relates to leadership dynamics at European level, with the overarching political priorities of the Commission being "green and digital" and an extensive focus on geopolitics and the EU's performance globally (I7). Moreover, it was mentioned that the innovation-oriented mindset and background of the European Commissioner for Internal Market helped to push digital policies, including the European Digital Identity proposal high on the political agenda (I4).

5 DISCUSSION

The EDIF has been considered an ambitious legislative proposal in many ways. Article 6a of the draft regulation requires Member States to issue a European Digital Identity Wallet under a notified eID scheme which, under Article 12b, private companies using strong authentication for online identification and 'very large platforms', are expected to accept [12]. The findings of this paper confirmed that the new proposal introduced at the beginning of P3 marks a major policy shift in the European digital identity policy. When looking back at the first two years of the von der Leyen Commission, few policy proposals and achievements in the digital realm exercise such a directly visible impact on the daily life of citizens. The European digital identity's impact will be felt on a range of topics touching every citizen including data protection, control and privacy. Despite these prospects, the proposal only made its appearance in the public sphere in early 2020.

By taking into account temporal processes for Hpi, we are able to provide an answer to our research question. We found that the reframing of the eIDAS Regulation with the incumbent Commission's digital policy priorities was largely responsible for policy punctuation. We also identified other contributing factors pushing the EDIF to the top of the policy agenda. The digital transformation of society and its acceleration triggered by the COVID-19 pandemic acted as a momentum for policy-makers to realize the need of providing citizens with secure, digital and user-centric conditions. The technological developments in the field, such as the concept of SSI and verifiable credentials, cannot be neglected. Neither can the political leadership under which digital policies are either slowed down or pushed ahead. So far, the role of technology and innovation in the policy agenda-setting process remains an interesting and under-researched phenomenon in the analysis of digital policy research. This compels us to make several observations, which we did not set out to analyze within the scope of this investigation, but could be worth exploring in further research.

First of all, the European digital identity's alignment with the Commission's digital priorities stands in contrast to its struggle to find its place on the political agenda until the beginning of the COVID-19 crisis in Europe. This raises the question of how many other such proposals with significant impact are waiting at the edge of the political agenda, due to dynamics that Rhinard [28] described as *'crisisification'* of European policy-making [28]. A second observation is linked to the staggering speed - by European standards - at which the European Digital Identity Proposal was submitted. This policy punctuation demonstrates that, in contrast to past records of EU legislative processes, the Commission and the European Council can, when the right circumstances are present, act fast, decisively and ambitiously. Third, one of the key lever for policy punctuation highlighted by PET is venue-shopping. While Princen [27] found evidence that some venue-shopping can occur at EU-level, we could not identify any such dynamic leading to policy punctuation in this particular case. What we found however, is that the venue has shifted through the change of Commission leadership, leading to a de facto different venue with different priorities. These findings reinforce the significance of comparative analysis on venue-shopping in the USA, China and the EU [35] and feeds into the need for furthering research on the impact of the EU's institutional policy venue structures.

6 CONCLUSIONS

This article adopted a PT approach to trace the policy process dynamics that led to the speedy introduction of the EDIF proposal. The findings of our analysis validated both hypotheses. We found that political mechanisms during the von der Leyen mandate (P2) explain the process through which the new Proposal came to be. In fact, P2 was marked by a sudden urgency for a European digital identity aligned with the Commission's digital priorities (digital sovereignty, data control, Digital Single Market and competitiveness). In addition to that, other explanatory variables not captured by our hypotheses emerged during the analysis. This leads us to this study's main limitations.

Mapping our results against Collier's [8] PT test for causal inference highlights our first limitation: an affirmed but weak causal inference. Our analysis confirmed the policy image hypothesis, but it was not possible to completely eliminate rival hypotheses. This is visible in the three additional factors that were involved in the agenda-setting process described in section 4.3. Identifying causal mechanisms using PT is however subject to the typical caveat that hypothesis testing in social science rarely yields 'doubly decisive' causal inferences. This limitation could be weakened with a comparative follow-up study. Second, PET offers little explanatory value regarding the interaction between policy and technological developments in digital policy-making. Our findings on the digital acceleration through COVID-19, the development of the concept of SSI, and the influence of a techno-enthusiastic policy venue did not match any theoretical explanation in our study.

To set off this limitation, future research could be dedicated to the interplay between politics and technology against the background of PET. To this end, it can be helpful to borrow concepts from the Science and Technology Studies discipline. In answering our research question we found that rather than a single exogenous triggering event such as an innovation, a strategy to attract attention is the reconfiguration of the policy image through institutionalized policy priorities of a government's mandate. Hence, a constructivist approach [3] lends itself as an adequate theoretical point of departure to study technology, such as digital identities, in a broader societal and institutional context [34]. However, in the evolution of digital identity management, the use of a digital wallet and verifiable credentials [29] was likely not initiated by policy choices alone, a dynamic that can be confirmed with Orlikowski's [25] structuration model of technology [34]. There is a clear elective affinity between policy issues and innovation in which policies influence and are influenced by technological innovation at both the problem and the solution stage of the policy process. For the punctuation of an equilibrium in the field of public policy, the concept of technological momentum, where the interaction between policy issues and technology are mutually reinforcing, appears to be appropriate [17]. This hybrid concept between 'soft' technological determinism and social constructivism encompasses the interest of governments to keep pace with technological innovation and its geopolitical implications, while recognizing institutional, cybernetic legacies [14, 16]. Questions such as, why a specific technology problem and not others attracts the attention of policy-makers, or why a specific technology is considered a potential solution to the policy problem, could be studied.

This would be an opportunity to empirically substantiate the role of technological innovations in public policy agenda-setting, by, for instance, looking into national contexts. An example could be Estonia's digital governance model and its chapter on digital identity policy as a hybrid product of government and private initiatives. Such discussions offer various avenues for future research in the fields of technology and public policy to reveal practical implications for the digital transformation of public services and governments.

ACKNOWLEDGMENTS

This research was supported by PayPal and the Luxembourg National Research Fund FNR, Luxembourg (P17/IS/13342933/ PayPal-FNR/Chair in DFS/Gilbert Fridgen). We thank Cristina Timón López who shared with us her knowledge and expertise to validate and clarify specific legal understandings in the research paper.

REFERENCES

[1] Frank R. Baumgartner and Bryan D. Jones. 1993. Agendas and Instability in American Politics. University of Chicago Press, Chicago.
[2] Derek Beach. 2017. Process-Tracing Methods in Social Science. Oxford Research Encyclopedia of Politics (2017).
[3] Wiebe E. Bijker, Thomas Parke Hughes, and Trevor Pinch (Eds.). 1987. The Social construction of technological systems: new directions in the sociology and history of technology. MIT Press, Cambridge.
[4] Paul Cairney. 2012. Understanding Public Policy: Theories and Issues. Palgrave Macmillan, New York. OCLC: ocn747232747.
[5] Edoardo Celeste. 2019. Digital Constitutionalism: A New Systematic Theorisation. Intl. Review of Law, Computers & Technology 33, 1 (2019).
[6] Cristiano Codagnone, Giovanni Liva, Laura Gunderson, Emanuele Rebesco, and Gianluca Misuraca. 2021. Europe's Digital Decade and Autonomy. Study Requested by the ITRE Committee. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
[7] Cristiano Codagnone, Giovanni Liva, and Teresa Rodriguez de las Heras Ballell. 2022. Identification and Assessment of Existing and Draft EU Legislation in the Digital Field. Study for the Special Committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
[8] David Collier. 2011. Understanding Process Tracing. Political Science and Politics 44, 4 (2011).
[9] European Commission. 2019. Overview of pre-notified and notified eID schemes under eIDAS - eID User Community. https://ec.europa.eu/digitalbuilding-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[10] European Commission. 2020. Shaping Europe's Digital Future. Technical Report. Publications Office of the European Union, Luxembourg.
[11] European Commission. 2021. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade.
[12] European Commission. 2021. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.
[13] Giovanni De Gregorio. 2021. The Rise of Digital Constitutionalism in the European Union. International Journal of Constitutional Law 19, 1 (2021).
[14] Michael De Percy and Heba Batainah. 2021. Identifying Historical Policy Regimes in the Canadian and Australian Communications Industries using a Model of Path Dependent, Punctuated Equilibrium. Policy Studies 42, 1 (2021).
[15] European Commission, Directorate-General for Communications Networks, Content and Technology. 2020. Inception Impact Assessment: Revision of the eIDAS Regulation – European Digital Identity (EUid). Technical Report.
[16] Luciano Floridi. 2020. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology 33, 3 (2020).
[17] Thomas Parke Hughes. 1994. Technological Momentum. In Does Technology Drive History?: The Dilemma of Technological Determinism. MIT Press, Cambridge.
[18] Marijn Janssen, Paul Brous, Elsa Estevez, Luis S. Barbosa, and Tomasz Janowski. 2020. Data Governance: Organizing Data for Trustworthy Artificial Intelligence. Government Information Quarterly 37, 3 (2020).
[19] Bryan D. Jones and Frank R. Baumgartner. 2012. From There to Here: Punctuated Equilibrium to the General Punctuation Thesis to a Theory of Government Information Processing: Jones/Baumgartner: Punctuated Equilibrium Theory. Policy Studies Journal 40, 1 (2012).
[20] Adrian Kay and Phillip Baker. 2015. What Can Causal Process Tracing Offer to Policy Studies? A Review of the Literature. Policy Studies Journal 43, 1 (2015).
[21] Harold Dwight Lasswell. 1956. The Decision Process: Seven Categories of Functional Analysis. Bureau of Governmental Research, College of Business and Public Administration, University of Maryland, College Park.
[22] Tambiama Madiega. 2020. Digital Sovereignty for Europe. Briefing: EPRS Ideas Paper Towards a More Resilient EU. European Parliamentary Research Service, Luxembourg.
[23] Philipp Mayring. 2014. Qualitative Content Analysis: Theoretical foundation, Basic Procedures and Software Solution. Open Access Repository.
[24] Mar Negreiro. 2021. Updating the European Digital Identity Framework. Briefing: EU Legislation in Progress. European Parliamentary Research Service, Luxembourg.
[25] Wanda J. Orlikowski. 1992. The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science 3, 3 (1992).
[26] Sebastiaan Princen. 2011. Agenda-Setting Strategies in EU Policy Processes. Journal of European Public Policy 18, 7 (2011).
[27] Sebastiaan Princen. 2013. Punctuated Equilibrium Theory and the European Union. Journal of European Public Policy 20, 6 (2013).
[28] Mark Rhinard. 2019. The Crisisification of Policy-making in the European Union. Journal of Common Market Studies 57, 3 (2019).
[29] Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. 2021. Digital Identities and Verifiable Credentials. Business & Information Systems Engineering (2021).
[30] Oisín Tansey. 2007. Process Tracing and Elite Interviewing: A Case for Non-Probability Sampling. Political Science and Politics 40, 4 (2007).
[31] James L. True, Bryan D. Jones, and Frank R. Baumgartner. 2007. Punctuated-Equilibrium Theory: Explaining Stability and Change in Public Policymaking. In Theories of the Policy Process (2 ed.). Westview Press, Boulder.
[32] Mari Tuominen and Solène Festor. 2021. Establishing a Framework for a European Digital Identity. Briefing: Initial Appraisal of a European Commission Impact Assessment. European Parliamentary Research Service.
[33] Jeroen Van der Heijden, Johanna Kuhlmann, Evert Lindquist, and Adam Wellstead. 2021. Have Policy Process Scholars Embraced Causal Mechanisms? A Review of Five Popular Frameworks. Public Policy and Administration 36, 2 (2021).
[34] Linda Weigl, Tom Josua Barbereau, Alexander Rieger, and Gilbert Fridgen. 2022. The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. In Proceedings of the Hawaii International Conference on System Sciences 2022.
[35] Stefanie Weil. 2017. Policy-Making Compared: China, the EU, and the US. In Lobbying and Foreign Interests in Chinese Politics. Palgrave Macmillan US, New York.
[36] Shoshana Zuboff. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology 30, 1 (2015).
[37] Svein Ølnes, Jolien Ubacht, and Marijn Janssen. 2017. Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. Government Information Quarterly 34, 3 (2017).

A APPENDICES

A.1 Interviews

Table 1: Interview Partners

#	Position	Affiliation	Interview Date
I1	Policy Officer	Government Institution	03.03.2022
I2	Policy Officer	Government Institution	16.03.2022
I3	Head of Unit	Government Institution	18.03.2022
I4	Head of Unit	Government IT Centre	18.03.2022
I5	ICT Consultant	Cybersecurity Consultancy	22.03.2022; 29.03.2022
I6	Researcher	University	29.03.2022
I7	Head of Unit	Government Institution	29.03.2022
I8	Legal Advisor	IT Services and Consulting Company	29.03.2022
I9	Director	IT Services Company	30.03.2022
I10	Director	IT Security Company	04.04.2022

A.2 Policy Documents

Table 2: Policy Documents Information

#	Document name	Publication
D1	Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market	06.2012 (P1)
D2	Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market	07.2014 (P1)
D3	(Juncker) Political Guidelines for the next European Commission 2014-2019 - A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change	07.2014 (P1)
D4	Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU	10.2017 (P1)
D5	(Von der Leyen) Political Guidelines for the next European Commission 2019-2024 - A Union that strives for more - My agenda for Europe	10.2019 (P2)
D6	Shaping Europe’s Digital Future	02.2020 (P2)
D7	Council conclusions on shaping Europe’s digital future	06.2020 (P2)
D8	Special meeting of the European Council (1 and 2 October 2020) - Conclusions	10.2020 (P2)
D9	Berlin Declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the Council	12.2020 (P2)
D10	2030 Digital Compass: the European way for the Digital Decade	03.2021 (P2)
D11	Impact assessment report accompanying the document Proposal for a Regulation amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity	06.2021 (P2)
D12	Proposal for a regulation amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity	06.2021 (P3)

USER-CENTRICITY AND PUBLIC VALUES IN EGOVERNMENT: FRIEND OR FOE?

Research Paper

Linda Weigl, University of Luxembourg, Luxembourg, Luxembourg, linda.weigl@uni.lu

Alexandre Amard, University of Luxembourg, Luxembourg, Luxembourg, alexandre.amard@uni.lu

Hanna Marxen, University of Luxembourg, Luxembourg, Luxembourg, hanna.marxen@uni.lu

Tamara Roth, University of Luxembourg, Luxembourg, Luxembourg, tamara.roth@uni.lu

Liudmila Zavolokina, University of Zurich, Zurich, Switzerland, zavolokina@ifi.uzh.ch

Abstract

In their delivery of services, public administrations seek to develop a 'citizen-centric' approach. Concomitantly, user-centricity is emerging as a widely accepted construct for Web 3.0 applications supporting the digital interaction between service providers and recipients. The digitalization of public services can positively impact important public values, such as efficiency and transparency. However, the digital divide highlights that information and communication technologies can simultaneously neglect public needs. This begs the question of whether user-centricity reflects or conflicts with public values. To answer this question, we present a systematic review of existing literature on user-centricity and public values. The contribution of this paper is an extended taxonomy of public values for user-centricity, as well as recommendations for public policy to address conflicts between public values and user-centricity.

Keywords: User-centricity, citizen-centricity, public values, eGovernment, literature review.

1 Introduction

In eGovernment, initiatives face many problems that arise from what Heeks (2003) defines as the 'design reality gap.' That is, societal and institutional realities are so far apart that their forced combination in eGovernment projects inevitably leads to discrepancies that need to be resolved. At the same time, these projects strongly rely on the willingness and readiness of citizens to use proposed technical innovations. The dependency on citizens makes eGovernment projects particularly cumbersome as they require an assessment of needs beyond institutional levels (van Deursen et al. 2006; Heeks 2003).

This particularly extends to 'citizen-centric' approaches, which public administrations have already started to develop in the analog world of services. These approaches are defined by "policy and expenditure choices that respond to and anticipate citizen needs" (OECD 2019). More specifically, they attempt to enhance civic engagement and provide accessible information and services to citizens (Cooper et al. 2006; Thomas 2013). This also includes the consideration of citizens' needs at the design stage of services and products. While citizens' needs may appear volatile and whimsical, they are allocated to more general public value categories (Karunasena and Deng 2011). Bannister et al. (2014) define public values as "a mode of behavior [or] a way of doing things […] that is held to be right […] by the public, citizens or the so-called 'reasonable man'" (p.120). Such values, encompassing, for instance, social inclusion, equality, fairness, or transparency, are typically integrated into citizen-centric government approaches (Bannister 2000; Karunasena and Deng 2011). Citizen-centricity thus can serve the public good and therefore reflects public values.

With the use of new technologies for public services in the Web 3.0 era (Dwivedi et al. 2011), governments increasingly focus on citizens as users (Codagnone et al. 2020). Consequently, 'user-centricity' evolved to describe approaches to design applications supporting digital interactions between citizens and public administrations. User-centricity epitomizes a widely accepted principle in the design and development of digital services. It is commonly defined as "a design philosophy in which the needs and expectations of the end user of an interface are the center of focus" (Kurdi et al. 2010). Some user-centric approaches[1] imply user control, i.e., the capability of users to manage personal data (Eap et al. 2007). This approach presumes that citizens possess sufficient digital skills to navigate information and make responsible decisions based on available data, which is often far from reality. Instead, it epitomizes a 'reality gap' that becomes visible in the persistence of the digital divide, a social phenomenon where "significant minorities of the population are effectively denied access to a technology […] thought to be open to anyone" (Robinson et al. 2003). In other words, the 'needs and expectations of end users' of different societal groups are not equally considered or addressed (Heeks 2003; Helbig et al. 2009).

Thus, the representation of public values in citizen-centricity may not hold for user-centricity. In fact, the digital-divide literature suggests that user-centric ICT (Information and Communications Technology) can even negatively affect values like social inclusion (Ferro et al. 2011; Norris and Norris 2001). This begs the question of whether user-centricity can coexist with or is related to public values and, therefore, fit for use in eGovernment services.

The urgency to approach this question increases with the parade of new technologies, such as blockchain, spreading into many aspects of society, including governments' way of delivering services (Ølnes et al. 2017). User-centricity, in this regard, is an important paradigm in the design of digital services to enhance the collaborative relationship between service providers and users. Yet, if user-centricity and user-centric technologies only center around a subset of citizens' needs and preferences, eGovernment initiatives might fail. This puts pressure on policy-makers to implement and regulate user-centric technologies in the right way. We thus pose our research questions as follows:

RQ1: How is user-centricity in the context of eGovernment services aligned with public values?

RQ2: Which public values conflict with user-centricity in the context of eGovernment services and why?

We present a systematic literature review on user-centricity and public values to provide a tentative answer to the research questions. The contribution of this paper is an extended taxonomy of public values for user-centricity based on current publications. Moreover, we introduce potential conflicts between public values and user-centricity and formulate policy recommendations to address these conflicts. As such, our paper aims to underpin the importance of public value considerations for the design and implementation of successful Government-to-Citizen approaches. This enriches existing research by not only deconstructing the meaning of user-centricity for public values, but also by elaborating on associated conflicts. More specifically, our paper may serve as a foundation for further research on public-value-based user-centric approaches in eGovernment 3.0 and new technological applications such as decentralized digital identities. In doing so, this study approaches a research gap by analyzing the most recent literature on public values and user-centric eGovernment and by identifying both synergies and conflicts between the two. For eGovernment practitioners, this paper offers explanatory value to the question of how user-centric approaches fit into the value proposition of democratic eGovernment initiatives.

The remainder of the paper is structured as follows. To highlight the relevance of user-centricity for eGovernment initiatives, we elaborate on the concept of user-centricity in connection with public values and eGovernment in section 2. Section 3 outlines the method of our systematic literature review. We then analyze our data in section 4. Finally, we discuss our results and conclude.

[1] Please, note that we use 'user-centric approaches', 'user-centric design' and 'user-centricity' as synonyms, even though one can distinguish between them. For the purpose of this study, we do not differentiate between 'user-centered'/'user-centeredness' and 'user-centric'/'user-centricity'.

2 Conceptual background

2.1 User-centricity

User-centric approaches emerged in the 1980s in human-computer interaction (HCI) research and were recognized with the rise of software development projects. As commonly understood, user-centricity considers users' needs, expectations, skills, preferences, and perspectives (Kurdi et al. 2010; Jarke 2021). User-centric approaches were broadly accepted and used by software designers in various domains, producing X-centered design: like healthcare with patient-centered design (Rodriguez et al. 2007), workplace with employee-centered design (Spurlock and O'Neil 2009), or public administration with citizen-centric design (van Velsen et al. 2009). User-centricity in the context of systems development can be seen as a multidimensional concept composed of four aspects (Iivari and Iivari 2011): (1) User-centricity as *user focus*, (2) User-centricity as *work-centeredness*, (3) User-centricity as *user involvement*, (4) User-centricity as *system personalization*.

Each of these four aspects provides a different complementary dimension to the concept of user-centricity. First, *user focus* relates to a common understanding of addressing users' needs determined by their activities or tasks, considering their characteristics (such as skills or personal preferences). Second, *work-centeredness* reflects the understanding of users' work activities, the context of use, work practices and helps to model the work domain holistically. Third, *user involvement* reflects the 'importance and relevance users attach to a given system' (Iivari and Iivari 2011). Here, the authors provide differentiation between user involvement and user participation. The latter is a case of user involvement, in which users actively participate in the design process. In product development, companies that produce IT solutions see user involvement as an indicator of the product's success on the market. Fourth, *system personalization* reflects adaptability or adaptivity of the system's content structure, presentation, and functionalities to each user's preferences or behaviors.

Such a multidimensional view provides a better and more holistic understanding of user-centric approaches in designing IT products in the market. However, in the context of eGovernment services, which has a strong focus on and the obligation to create public value, they may manifest differently, be incomplete or even clash with certain public values. While user-centered design approaches proved useful and beneficial in software design, they are criticized for ignoring such aspects as sustainability, societal impacts, and consequences (Sevaldson 2018). Therefore, we apply the public value perspective to examine how different dimensions of user-centricity incorporate public values, which are at the heart of the design of eGovernment services. Our study addresses this critique – at least partly – by including the public value perspective and demonstrating how far user-centricity is both aligned and conflicting with public values.

2.2 Public values in eGovernment

"Rarely has anyone explicitly addressed the question of why the public sector invests in IT, and of what it is hoping to achieve if not increased competitive advantage" (Wyatt 1991, p.25). This issue was pointed out in 1991 to inquire into the rationale behind governments' effort to digitize public services. An answer to this question could be that eGovernment services, as opposed to commercial service providers, pursue objectives that go beyond profitability and growth. In general, democratic governments depend on public administration for the daily management and delivery of public services and policies. Public administrations, thus, "have an inherently democratic mission and must rely on support from citizens and institutions of government for their viability" (Ventriss et al. 2019, p. 276).

Therefore, a more trusted, efficient, inclusive and transparent governance is typically a core objective of eGovernment to make government services more convenient (Bekkers and Homburg 2007; Fountain 2001). Consequently, the question of how the use of ICT for public services relates to the values that support these objectives becomes more critical (Bonina and Cordella 2009; Grimsley and Meehan 2007).

To define 'public values' and capture the relationship between these values and eGovernment, Bannister (2000) distinguishes between *values*, *value*, and *benefits*. *Values* represent a normative consensus that manifests as a specific mode of behavior. Many individuals share the same belief in certain values, such as, for instance, fairness and impartiality. On the other hand, *value* can be described as the worth assigned to an outcome or a service that conforms to specific values. Suppose some individuals agrees that all citizens should be treated fairly and impartially when using electronic public services. In that case, these individuals will place value on IT systems that do not produce bias or discrimination. Finally, *benefits* are an operationalization of the attached value to a service, product, or outcome. For example, when governments assess an IT system based on its ability to conform to the specific values of fairness and impartiality, both underrepresented groups and governments themselves will benefit from the outcome. In other words, "value is what we perceive; benefit is what we receive" (Bannister 2000, p.34).

It is important to differentiate between commercial and public service providers' perceptions of value and benefits. While motivation and complexity are two diverging elements in public and private service models, the most fundamental contrast is the relationship between the service provider and the recipient (Bannister 2000; Jos and Tompkins 2009). In a commercial setting, customers usually have a free choice between products and services and the possibility of opting out to cancel a transaction. On the other hand, governments are a monopoly supplier and citizens do not have the option to switch the provider or refuse a service. Hence, the acceptance and success of eGovernment services relies on governments' relations with citizens. In the New Public Management (NPM) approach, governments thus focus on citizens as customers by mimicking private sector management models and adopting market-based mechanisms (Ferlie et al. 1996; Pollitt and Bouckaert 2003). NPM, however, exhibits a mainly scientific and decision-centric, rather than user-centric accentuation (Bason and Austin 2021). When these efforts resulted in increased administrative complexity and various other dysfunctional side effects, the Digital Era Governance (DEG) emerged as an attempt to re-aggregate public services around users' needs (Dunleavy 2005). This dialectic of public administration governance approaches requires further exploration of user-centricity and its alignment with public values. Bannister et al. (2014) developed a taxonomy of public service values for IT (Table 1). Their study identifies twenty-eight administrative public values and categorizes them into three types: duty-oriented, service-oriented, and socially oriented. *Duty-oriented values* include values related to the duties of the civil servant to the government. *Service-oriented values* reflect the responsibility of the civil servant to provide high-quality service to citizens as customers of public administration. Finally, *socially oriented values* exhibit a broader set of social goods. This taxonomy of public values has become well-established and frequently used in studies that examine the impact of ICT in eGovernment. Our study leans on the presented public values to examine their relation to user-centricity in the existing literature.

Duty-oriented	**Service-oriented**	**Socially oriented**
Responsibility to the citizen Responsibility to the elected politicians Proper use of public funds Compliance with the law Efficient use of public funds Integrity and honesty Facilitating the democratic will Accountability to government Economy/parsimony Rectitude	Service to the citizen in his or her different roles Respect for the individual Responsiveness Effectiveness Efficiency Transparency	Inclusiveness Justice Fairness Equality of treatment and access Respect for the citizen Due process Protecting citizen privacy Protecting citizens from exploitation Protecting citizen security Accountability to the public Consulting the citizen Impartiality

Table 1. A proposed taxonomy of public values for assessing the impact of ICT (Bannister et al. 2014).

3 Method

The objective of our systematic review is to examine the reflection of public values in the concept of user-centricity. Methodologically, we followed Kitchenham's five-step approach, a well-established methodology in information systems (vom Brocke et al. 2015). We chose this concept-centric approach over other literature review approaches, such as narrative, critical or realist (Paré et al. 2015), to ensure replicability, rigor, and objectivity of the review process for two widely used concepts – public values and user-centricity – in government literature (Boell and Cecez-Kecmanovic 2015). This approach consists of (1) the identification of relevant publications, (2) the selection of relevant publications, (3) the evaluation of the publications' quality, (4) the extraction and evaluation of data, and (5) the aggregation and interpretation of data.

First, to identify relevant publications, we conducted a keyword search across five databases (IEEE Xplore, ScienceDirect, SAGE Journals, SCOPUS, and Taylor & Francis). We combined the keywords with the Boolean operators AND OR. To avoid language bias, we used speech and spelling variants of our key concepts, such as 'user-centricity', 'user-centric', 'user centric' and 'user-centered'.

We applied further criteria regarding publication types, language and publication year (see Table 5 in the appendix). As indicated in Table 5, we targeted publications from various disciplines, as long as they contained non-technical considerations and implications relevant for the analysis. Literature centering around eGovernment 1.0 and early eGovernment 2.0 was not included in the review by considering only articles published in 2012 or later. Naturally, papers needed to be screened manually in order to ensure that outdated eGovernment applications were not part of the analysis. All identified literature was exported into the bibliographic reference manager Zotero. We identified 6937 potentially relevant scientific contributions after having removed duplicates and books[2].

The search strings used for the systematic literature review were the following:

1. "User-centricity" **AND (**"Government" **OR** "Public Sector" **OR** "Public Administration"**)**
2. "Citizen-centricity" **AND (**"Government" **OR** "Public Sector" **OR** "Public Administration"**)**
3. "Customer-centricity" **AND (**"eGovernment" **OR** "Digital Government" **OR** "Digital Transformation" **OR** "Transformative Government"**)**
4. "Values" **AND (**"eGovernment" **OR** "Digital Government" **OR** "Digital Transformation" **OR** "Transformative Government"**)**

After this initial and more general pre-selection of literature, we continued with the second step (selection) and third step (evaluation) of Kitchenham's approach, using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol by Moher et al. (2009) (Figure 1). This protocol enables transparency, easy replicability, and verifiability of the results (Liberati et al. 2009). PRISMA consists of four phases – (1) identification as in Kitchenham's (2004) model, (2) screening, (3) eligibility, and (4) inclusion. In the screening phase, we selected the 206 articles based on the titles in two independent groups. The Cohen's kappa coefficient of the inter-group reliability regarding this first selection round of .94 was "almost perfect", considering that 1 corresponds to a perfect fit (Cohen 1960). During this exclusion procedure, we re-applied our pre-defined search selection criteria (Table 5). As the heterogenous search tools of the respective databases also yielded studies which were not related to our key concepts, we had to re-assess the selection criteria manually regarding the topic and discipline of the articles. In a next step of the screening phase, we discussed the publications based on the abstract, again in two independent groups. In a first step, we reduced our selection to 136 articles with an inter-group reliability coefficient of .73 between the selectors. In the refinement stage, we grouped the 136 articles according to cases, time span of their data collection and central foci of the studies (Kitchenham 2004). Doing so allowed us to exclude further 19 publications, leading to 117 articles. These publications dealt with cases of digital transformation that we considered outdated (such as eGovernment 1.0) or did not focus on technologies in the public sector. Examples include studies that

[2] The search operators were usually applied to full text and metadata. However, in cases where our search yielded more than 700 publication results, we restricted the search fields to key words, abstract or introduction, depending on the available filters of each database.

analyzed social media, or government websites, as well as studies with survey data from before 2012. When retrieving full-text articles, we could not access 8 papers. This further reduced our number of studies to 109. Among this set of 109 articles, we selected 30 articles for our qualitative analysis. We selected these 30 articles (Table 6) based on their relevance and usefulness to analyze the reflection of public values in the construct of user-centricity as well as the publications' citations per year and the impact factor of their publication outlet for additional quality insurance (Coombes and Nicholson 2013). Fourth, for data extraction and analysis, we applied a mixed-methods approach using MAXQDA. For the qualitative part, we manually coded 30 papers in two separate coding teams employing a two-stage coding process of inductive and deductive coding (Saldaña 2013). That is, we first consulted literature on public values to derive a set of codes that we used to deductively identify principles of user-centricity in our literature as well as potential construct-related conflicts and implications for public values. Then, we complemented our initial codes with other codes as emerged during our analysis and assigned them to higher-level concepts (inductive coding). This led to overall 2791 codified statements organized in 72 first-order themes and 16 second-order categories (Miles et al. 2014). To identify potential conflicts, we marked respective codes and re-analyzed the coded statements, summarizing and aggregating our findings to the most salient conflict areas. To investigate the relationships between user centricity characteristics and public values, we performed a code relation analysis followed by a qualitative content analysis. The quantitative analysis allowed us to observe overlaps between the individual codes and thus the relationship between them. We subsequently carried out a qualitative coding query to investigate which of these relations were aligned and conflicting overlaps between public values and user-centricity.

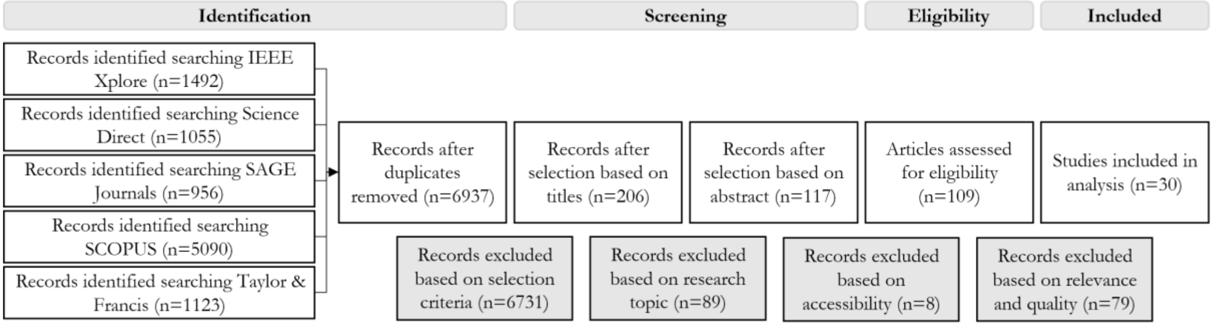

Identification
Screening
Eligibility
Included
Records identified searching IEEE Xplore (n=1492)
Records identified searching Science Direct (n=1055)
Records identified searching SAGE Journals (n=956)
Records identified searching SCOPUS (n=5090)
Records identified searching Taylor & Francis (n=1123)
Records after duplicates removed (n=6937)
Records after selection based on titles (n=206)
Records after selection based on abstract (n=117)
Articles assessed for eligibility (n=109)
Studies included in analysis (n=30)
Records excluded based on selection criteria (n=6731)
Records excluded based on research topic (n=89)
Records excluded based on accessibility (n=8)
Records excluded based on relevance and quality (n=79)

Figure 1. Study selection, assessment, and inclusion (PRISMA flow diagram).

4 Findings

This section reports our findings from the analysis of the selected research articles concerning user-centricity, citizen-centricity and public ICT values. First, we provide a descriptive analysis of our set of literature. Section 4.1 captures an overview of the newly identified public values. In 4.2, we outline the alignment of user-centricity with public values based on our qualitative analysis. Likewise, in section 4.3, we report our findings regarding public value conflicts with user-centricity.

In our selection of 30 articles, 24 were journal articles, 4 conference articles and 2 book chapters. Most journal and conference papers can be associated with information systems (25.00%), followed by electronic governments (21.43%) and public administration (17.86%) (based on the categorization from Pang et al. (2014)). The most common journal was Government Information Quarterly (3 articles). 4 articles were published between 2013 and 2014, 8 between 2015 and 2017, 11 between 2018 and 2020 and 5 in 2021. Most papers used surveys (25.00%) or literature reviews (25.00%) as methods, followed by case studies (15.63%), interviews (12.50%), analysis of existing data (6.25%) and content analysis (6.25%). Some articles used more than one method.

Table 2 illustrates the code co-occurrences between the three public value types (duty, service and socially oriented) and the three dimensions of user-centricity (user focus, user involvement and system personalization). Co-occurrences indicate only the overlap of two groups of codes (user-centricity and public values) and their sub-codes for a particular segment. To differentiate between value alignment and conflict, we carried out a qualitative analysis. The percentages in the table hence indicate the frequency of co-occurrences between a specific public value (e.g., trust) and a user-centric dimension (e.g., user focus) in a text segment per overall frequency of co-occurrences between public values and a specific user-centric dimension. For example, 4.60% of the code co-occurrences of user focus with public values are between user focus and trust. We did not find any reflection of work-centeredness, the fourth dimension of user-centricity in our analysis. This is because the reviewed literature considers users as citizens and public service recipients, while work-centeredness focuses on users' occupational roles in a professional context, which are not within the scope of this study. Therefore, we excluded it. Table 2 includes solely public values that occurred in our documents. We did not include values of Bannister's et al. (2014) taxonomy that were not represented in the selected literature.

4.1 Public values for user-centricity

We identified eight additional public values (Table 3) that may enrich the proposed types by Bannister et al. (2014). These values are (1) *legitimacy* and *representation* for the duty-oriented values, (2) *flexibility* for the service-oriented values, and (3) *accessibility*, *pluralism*, *trust*, *autonomy*, and *innovation* for the socially oriented values. We split *equality of treatment and access* into *equality* and *accessibility*. Moreover, we re-formulated *consulting the citizen* to *citizen involvement / consulting.*

Legitimacy, which has evolved as a determinant of eGovernment adoption besides novelty and usefulness, focuses on the question of whether eGovernment truly serves the public interest. Therefore, academic literature proposes civic engagement to create legitimate eGovernment (#1; #13; #14; #16; #18; #20). Corresponding bottom-up driven *citizen involvement* would enhance the legitimacy of public actors' decisions and activities in eGovernment. Current eGovernment systems rarely employ a bottom-up system design approach and often lack not only legitimacy, but also *representation* of different user groups (#13; #15; #19; #22). Different user groups have different preferences and needs. Therefore, a personalized system might provide the desired *flexibility* to account for the varying requirements of different user groups (#1; #2; #6; #13; #18; #20; #21). *Accessibility* appears to be a key component to user-centric service design (#3; #7; #9; #10; #17; #21; #24; #29). Accessible services help citizens better understand the underlying processes and feel represented by the proposed system (#2).

		Public values																						
		Duty-oriented						Service-oriented					Socially-oriented											
		Proper use of public funds	Facilitating the democratic	Accountability to government	Economy / parsimony	Legitimacy*	Representation*	Responsiveness	Effectiveness	Efficiency	Transparency	Flexibility*	Inclusiveness	Fairness	Equality	Protecting citizen privacy	Protecting citizen security	Accountability to the public	Citizen involvement /	Accessibility*	Pluralism*	Trust*	Autonomy*	Innovation*
User centricity	UF	1.92	0.77	0.38	1.53	0	3.83	0.77	3.07	7.66	5.75	0.77	5.36	1.15	2.68	3.83	3.83	6.13	14.94	18.77	5.75	4.60	3.07	3.45
	UI	0	5.11	5.84	0	2.19	0.73	2.92	1.46	4.38	6.57	1.46	2.92	1.46	1.46	5.84	5.84	4.38	25.55	11.68	2.92	3.65	2.92	0.73
	SP	0	3.81	10.48	0	0	0.95	1.90	0	3.81	6.67	4.76	4.76	1.90	2.86	2.86	2.86	2.86	25.71	10.48	5.71	3.81	2.86	0.95

*Table 2. Code co-occurrences between user-centricity and public values in %. UF: User focus, UI: User involvement, SP: System personalization. * Marks the public values which are not included in the taxonomy of Bannister et al. (2014).*

Duty-oriented	Service-oriented	Socially oriented
Proper use of public funds Facilitating the democratic will Accountability to government Economy / parsimony Legitimacy* Representation*	Responsiveness Effectiveness Efficiency Transparency Flexibility*	Inclusiveness Fairness Equality Protecting citizen privacy Protecting citizen security Accountability to the public Citizen involvement / consulting Accessibility* Pluralism* Trust* Autonomy* Innovation*

*Table 3. Extended taxonomy of public values for user-centricity. * Marks the public values which are not included in the taxonomy of Bannister et al. (2014).*

This also encourages the value of *pluralism* as even the needs of marginalized groups might be heard and included (#1; #4; #12; #17; #19; #29; #30). Despite all aspirations to *equality* and *pluralism,* the *trust* in government services may also not be tarnished (#4; #9; #15; #17; #21; #23; #25; #26; #28; #30). This particularly refers to the application of *innovative* systems (#1; #29). *Innovation* and the therewith associated perception of novelty is an important determinant of technology acceptance, yet also the greatest weakness when it comes to *trust* (#3; #23; #29). New systems and new roles require citizens to rethink known structures and may lead to insecurities that impair institution-based trust in governments (#11; #17). Finally, citizens that depend on government services may be given more *autonomy* in their interaction with public administrations as the digital exchange of personal data is core the eGovernment services (#28; #30). *Autonomy*, in this context, embodies a value related to the ethical use of citizen data in the public sector and enables individual data control (#4; #9; #17; #26).

4.2 Alignment between user-centricity and public values

This section seeks to answer RQ1, namely, how user-centricity in eGovernment services is aligned with public values. In doing so, we evaluated our findings regarding the reflection of public values in the concept of user-centricity with qualitative content analysis (complex coding query).

User focus. Our code relations and qualitative analysis revealed that the *user focus* dimension is particularly aligned with *efficiency*, *citizen involvement* and *innovation*. User-centric approaches enable an *efficient*, cost- and time-saving interaction between users and service providers (#3; #7; #9; #13; #15; #22; #23; #28). As user-centric design focuses on users' needs and preferences, one of the main goals is to reduce the administrative burden and make services more intuitive and convenient (#17; #20). Further, many scholars indicate that with the increase in efficiency, user-centric approaches may stimulate *citizen involvement* (#3; #15; #21). This is especially possible with collaborative, interactive and participatory platforms that "transform political communication of citizens with the public sector in a digital manner as a much more cost-efficient and, arguably, even trust generating form of governance" (#15, p.2). We found *innovation* as a public value to be aligned with user-centricity, since it is a strong enabler for user satisfaction and, therefore, users' decision to adopt and accept digital technologies for government services (#2; #23).

User involvement. For *user involvement,* the strongest alignment occurs with *citizen involvement, facilitating the democratic will,* government *transparency for users* and *accountability to the public*. User involvement appeared to be directly related to *citizen involvement*, a term we deduced from the original value of *consulting the citizen* (#1; #2; #4; #8; #18; #19; #22; #28). Our analysis indicated that user-centric design is mostly amplified by "participatory and action-oriented" design (#21, p.41). The goal is to consider users' needs and preferences in the design stage of services, avoid top-down decisions and address design-reality gaps (#19; #21). In consequence, citizen involvement inevitably *facilitates the democratic will*, as the digital interaction of citizens with governments extends citizens' civic and political involvement and influence (#19; #23; #28). These democratic, participatory processes, in turn, allow for greater government *transparency* (#2; #3; #4; #9; #25; #26). *Transparency*, notably, leads "to a better-informed citizenry" (#22, p.3) and it is argued that "well-informedness" is a cornerstone for democracy and a fundamental component for public values (#28, p.7). This supports our fourth value alignment in this dimension, which highlights that citizen-centric approaches in eGovernment "help to reduce bureaucracy in governmental offices, stimulate citizens' participation in decision-making processes, and increase the transparency and *accountability* of governmental offices" (#3, #10, #16).

System personalization. Finally, *system personalization* is primarily aligned with *citizen involvement* and *flexibility*. As with the other two dimensions of user-centricity, system personalization is aligned with *citizen involvement* because the latter is a requirement for the former. In other words, governments need to collect information on citizens' preferences to design user-centric systems accordingly (#6; #22; #27; #28). Therefore, personalized and cutsomized services require civic engagement and participatory design to accurately and flexibly tailor the design to individual needs and preferences (#12; #13). In this context, we found system personalization to be well aligned with *flexibility* (#4; #6; #18). In order to meet the requirements of personalization, governments need to provide flexible services to better cater to citizens' preferences (#16; #18).

4.3 Conflicts between user-centricity and public values

To answer RQ2, namely, which public values conflict with the concept of user-centricity in the context of eGovernment services and why, we identified a total of seven conflicts between the three user-centricity dimensions and public values (Table 4).

Value conflict	User focus	User involvement	System personalization
Duty oriented	- Representation	- Accountability to government	
Service oriented	- Transparency		
Socially oriented	- Inclusiveness, pluralism and accessibility	- Inclusiveness	- Equality and pluralism - Autonomy

Table 4. Summary of conflicts between user-centricity and public values.

User focus. In the user focus dimension, three conflicts emerged. The first one occurred with the public value *representation*. This conflict is based on the premise that citizens and governments have diverging interests and needs and that governments cannot represent users' needs to the extent prescribed by user-centricity (#4; #11; #17; #19; #30). Central to this claim is that governments focus on their accountability as defined by law or on "fulfilling the international requirements rather than trying to understand the needs of their users" (#11, p.1). In consequence, they are obligated to offer comprehensive information and adhere to specific legally defined standards. This explains the well-known bureaucratic and inflexible procedures, which mostly do not align with users' preferences, such as simplicity, efficiency and anonymity (#17; #22). A second conflict concerns a trade-off between the focus on citizens' preferences and *transparency* (#4; #13; #17). On the one hand, user involvement and system personalization are aligned with *transparency for the user* because they enable user involvement in the design of services according to individual preferences. Yet, *transparency for the service provider*, that is the government, appears to be conversely affected. This conflict arises through user empowerment and the concomitant transfer of control over their personal data and information (#26; #28). While this rightfully enhances user privacy, it also challenges governments' access to non-privacy-restricted and non-confidential, so-called open data, which can support public oversight and help to reduce corruption

(#4; #16). We detected an additional critical conflict between user focus and the values of *inclusiveness*, *pluralism,* and *accessibility*. Pluralism, in this context, does not reflect classical pluralism as a political decision-making theory, but relates to a pluralistic society that tolerates and supports diversity. By definition, user-centricity focuses on users' needs in the design and application of technology (#3; #20; #21; #24; #29). Thereby, it is important to understand that users do not exclusively make up the presumed dominant group of young, educated, affluent, and technology-conscious people (#10). Instead, the needs of digitally less literate citizens, or people with restricted access to technological devices or connectivity, need to be especially taken into account (#10; #13; #17; #21).

User involvement. In the user involvement dimension, we detected two main conflicts. In the first conflict, which concerns *accountability to government*, researchers questioned the compatibility of the active participation of citizens on the one hand, and the accountability of public officials at the government level, on the other (#1; #8; #13; #16; #24). Public servants must comply with official standards and rules, which might not always match citizens’ knowledge and input. These standards also limit the involvement of citizens as they prevent the provision of individual workarounds by governments and the emergence of new and unregulated roles of citizens (#2; #17). Since user-centricity foresees the involvement of citizens exclusively through online channels and platforms, *inclusiveness* may be impaired (#15; #16; #24). That is, digitally less literate citizens may face neglect in participatory eGovernment initiatives (#1; #20; #21).

System personalization. In the system personalization dimension, our findings indicated a conflict with *equality* and *pluralism* (#1; #28). While user-centricity requires the adaptability of a system to specific user preferences, the personalization of a system for the public is often limited by the mandate and responsibility of governments to treat citizens equally. That is, governments often overrule individual needs to serve more general citizen needs. Many individual needs are irreconcilable with the required accountability of government services, so governments focus on the cumulative extract of needs, not the individual desire (#17). The final conflict refers to the trade-off between personalization and *autonomy* (König 2021). This conflict emerged in our findings mainly in the context of algorithmic systems for eGovernment. The issue is that personalized information risks nudging citizens in a certain direction, resulting in the (subconscious) loss of control over their decisions.

5 Discussion

The development of user-centric approaches in eGovernment implies changes for both the role of citizens and governments. On the one hand, public administrations are expected to digitalize their services and establish more efficient and transparent interactions with their citizens. On the other hand, citizens are expected to have sufficient digital skills to use electronic devices and have internet access. Moreover, decentralization and bottom-up driven initiatives require citizens to actively engage in the design of public services, and even policy-making. These dynamics imply the emergence of new public values that need to be considered for the concept of user-centricity in eGovernment.

This is particularly emphasized in the value alignments between user-centricity and socially- as well as service-oriented values, which we discovered in our analysis of the 30 selected publications. Duty-oriented values, however, were reported least in connection with user-centricity. Such findings underline the current design of user-centric eGovernment approaches. As our findings indicated, user-centric approaches try to minimize responsibilities or duties for users, while maximizing efficiency and user involvement to increase usability and uptake, and to avoid overwhelming citizens.

Although we primarily focused on the public value taxonomy provided by Bannister et al. (2014), the public administration literature and its branch in Public Value Management (PVM) offer various additional public value frames, “in which facts, values, theories, and interests are integrated” (Rein and Schön 1993). Nabatchi (2017), for example, suggests four public values frames: Political, legal, organizational, and market. The first two center around the “democratic ethos,” similar to Bannister et al.’s duty- and socially oriented values, and the latter appear as part of the “bureaucratic ethos”, corresponding to Bannister et al.’s service-oriented values. Rose et al. (Rose et al. 2015) cluster public values along four different value positions, which they define as the professionalism ideal, the efficiency ideal, the service ideal, and the engagement ideal. Again, parallels to Bannister et al.'s taxonomy can be derived. Despite these additional taxonomies and frames, values that emphasize social and service dimensions are most salient in current user-centricity literature on eGovernments.

A common ground for all public value frames is that public values are often ambiguous, hybrid, contrasting, and overlapping (Stoker 2006). This means that if user-centricity in eGovernment projects is conflicting with certain public values, this might be precisely because it is aligned with and fulfills other public values, highlighting clear signs of value pluralism (van der Wal and van Hout 2009). In our analysis, value conflicts with user-centric approaches appeared mainly in duty- and socially-oriented values and were seen less frequently in service-oriented values. These conflicts indicate that responsibilities of citizen in user-centric eGovernment approaches are not yet clear and that also contrasting views on the social dimension, for instance regarding digital literacy and digital inclusion, may encumber projects in practice for public managers. Therefore, analyses of competing public values in eGovernment research are a necessary step for the development and solidification of new frames and taxonomies, which help adjust to new technological developments in eGovernment, especially those that increasingly focus on users. Such taxonomies can in turn be a useful tool for eGovernment practitioners, such as public managers and officials, to assess new digital public services.

This paper contributes to this effort by extending Bannister's et al. taxonomy (2014), and by providing a set of administrative public values that can be used as foundation for research at the intersection of user-centricity, eGovernment 3.0, and public values. Our literature analysis further evidenced diverse value alignments as well as conflicts for our three dimensions of user-centricity – user focus, user involvement and system personalization. It should be mentioned that as with any literature synthesis, the findings of our literature review are a conceptual generalization and are not directly grounded in empirical reality. We synthesized insights from academic literature analyzing an array of different user-centric eGovernment applications. The identified value conflicts and alignments need to be empirically validated with individual use cases.

However, some implications for practice can be drawn. The conflicts between user focus and *inclusiveness*, *pluralism* and *accessibility*, as well as user involvement and *inclusiveness,* highlight that governments, other than commercial services providers, have the mandate to respect the needs of every citizen. Public administrations must design their services in a way that digitally less literate and other marginalized groups can use their services. Scholars widely agree that digital literacy and skills must be developed alongside general educational objectives (van Deursen and van Dijk 2009; Ferro et al. 2011). Based on these findings, our recommendation is to improve citizens' digital literacy and skills to "translate digital participation into positive outcomes" (Park and Humphry 2019). This could also include ad-hoc measures, such as the provision of IT assistants in libraries to help with public services online. The value conflicts between user focus and *representation* and *transparency*, user involvement and *accountability*, and system personalization and *equality* and *pluralism* all emphasize discrepancies between citizen and government needs. Citizens already perform bureaucratic tasks that they perceive as inconvenient, such as paying taxes or applying for social security benefits. Governments, on the other hand, are obliged to adhere to prescriptive models of organization. Blind reflection of descriptive user needs would only impair the organizational model (Park and Humphry 2019). While user-centric design focuses on "making users' tasks simple and easy" (Kotamraju and van der Geest 2012, p.7), governments must follow legal requirements regarding the presentation and formulation of information (Scott et al. 2016; Sorn-In et al. 2015). That is, the government is supposed to provide full information on a topic in a legally binding and acceptable manner. Yet, particularly in a digital environment, governments could make available additional and simplified explanations of legal documents to reduce the information overload for citizens. Moreover, other mandates of usability and functionality that do not touch binding regulation could be addressed at a technical design level (Sorn-In et al. 2015). Our literature review, therefore, strengthens the call on governments to proactively engage in understanding users' needs to create smart services (Bokayev et al. 2021; Ghosh Roy and Upadhyay 2017).

Overall, this paper may serve as a foundation for future studies on public-value-infused user-centric eGovernment 3.0. By analyzing literature on public values and user-centricity the study offers synergies and conflicts that may emerge through the adoption of user-centric eGovernment applications. As such, this research offers explanatory value to the question of how user-centricity may be positioned into the value proposition of democratic eGovernment initiatives.

6 Conclusion

This article set forth that successful user-centric eGovernment applications operate at the interface between fundamental public values and user-centricity. Thus, many public values are reflected in and aligned with user-centricity, adding new criteria to already existing taxonomies of user-centricity. On the other hand, user-centricity for eGovernment, as currently conceptualized in literature, also stands in contrast to some public values.

Since our article only synthesizes research evidence to uncover the relation between public values and user-centricity in eGovernment, our study suffers from several limitations. First, we determined the different public value categories only qualitatively and did not validate our results quantitatively. Showing how the different variables correlate with or describe the respective constructs factor-analytically could provide further indications on how public values are represented in user-centricity. Second, as is the case for most literature review studies, our analysis is limited to a certain selection of articles. Therefore, we might have missed papers, not fitting our search criteria.

Yet, we identified 30 influential academic contributions and corresponding results yield interesting insights of direct relevance to policy-makers. Our analysis provided an extension of the public value taxonomy tailored to user-centricity for eGovernment. In addition, we identified seven public value conflicts and provided two policy recommendations. Analogous to the widely studied conflict between needs of government and citizens, the conflict between public values and user-centricity results from design choices that include but do not unduly favor the desires of users. Yet, previous research focuses primarily on the lawfully required inclusion of minority groups or fundamentally different notions of the interaction between government and citizen (Carter and Bélanger 2005). Our paper extends this perspective by mapping public values against three dimensions of user-centricity. This leads to various conflicts between user perspectives and public values. In consequence, we recommend governments to be more proactive in asking for citizens' needs and assembling these needs into actionable and meaningful services. To not neglect marginalized and digitally less literate groups, governments could provide additional analog services or personal assistants.

Existing research streams on the digital divide acknowledge this phenomenon as a socially deeply engrained problem. Public values are guiding ethical criteria and principles to manage policies and services in a way that is acceptable by citizens and, as Bannister et al. (2014) put it, the "reasonable man" (p.120). In that sense, our extended public value taxonomy is a way to situate the problem of the digital divide, by, for instance, conceptualize it as hindering social inclusion, hampering equality, or prohibiting access and participation. It could be an interesting stream of research to further analyze the digital divide and its relation to public values for eGovernment. Moreover, we call for further research on how public values can be reflected in the technology design to benefit future eGovernment services and other public sector applications. It also remains to be determined to what extent citizens could and should be included in the design and provision of eGovernment services. In an effort to tackle those open questions, further studies could look into the ways public organizations are considering user-centricity and the potential conflicts with public values within their eGovernment strategies. For example, future research could incorporate grey literature emanating from public bodies that are in daily contact with end-users and complement it with findings originating from citizen-led initiatives. This would support both academics and authorities to better understand the dynamics at play and develop user-centric applications that exploit the synergies - and avoid the pitfalls - that exist between public values and user-centric approaches identified in this paper.

7 Acknowledgements

Supported by PayPal and the Luxembourg National Research Fund FNR, Luxembourg(P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen).

8 Appendix

	Inclusion criteria	Exclusion criteria
Discipline*	Information Systems Library and Information Science Public Administration Economics and Sociology Public Policy Business, Management and Accounting Marketing and Sales	Engineering Statistics Computer Science and Security Mathematics Natural and Life Sciences
Topics*	User-centricity; citizen-centricity; eGovernment; emerging technologies; public values	Architecture; systems, government portals and websites; social media; survey studies from 2012; value creation
Publication type	Book chapters Peer reviewed articles Doctoral theses Conference articles	Books Bachelor or Master theses
Language	English	Non-English
Publication year	2012 - 2021	Articles published before 2012

*Table 5. Literature search selection criteria. * Marks the criteria that had to be re-applied in the title and abstract selection procedure.*

#	Reference	#	Reference
1	Aschhoff and Vogel, 2018	**16**	König, 2021
2	Bason and Austin, 2021	**17**	Kotamraju and van der Geest, 2012
3	Bokayev et al., 2021	**18**	Kumar, 2019
4	Degbelo et al., 2016	**19**	Kyakulumbye et al., 2019
5	Ebbers et al., 2016	**20**	Larsson, 2021
6	Fröhlich, 2017	**21**	Mariën and Prodnik, 2014
7	Gable, 2015	**22**	Mossey et al., 2018
8	Ghosh Roy and Upadhyay, 2017	**23**	Mostafa and El-Masry, 2013
9	Gjermundrød and Dionysiou, 2015	**24**	Park and Humphry, 2019
10	Gupta et al., 2018	**25**	Parra and Libaque-Saenz, 2020
11	Hashim et al., 2020	**26**	Pérez-Morote et al., 2020
12	Hung, 2012	**27**	Purao and Wu, 2013
13	Ingrams, 2019	**28**	Scott et al., 2016
14	Janssen and Helbig, 2018	**29**	Sharma et al., 2016
15	Kassen, 2021	**30**	Sorn-In et al., 2015

Table 6. Overview of studies included in our systematic literature review.

References

Aschhoff, N., and Vogel, R. 2018. “Value Conflicts in Co-Production: Governing Public Values in Multi-Actor Settings,” *International Journal of Public Sector Management* (31:7), pp. 775–793. (https://doi.org/10.1108/IJPSM-08-2017-0222).

Bannister, F. 2000. “Serving the : A Proposed Model for IT Value in Public Administration,” *Southern African Business Review Special Issue on Information Technology* (4:2), pp. 33–40.

Bannister, F., and Connolly, R. 2014. “ICT, Public Values and Transformative Government: A Framework and Programme for Research,” *Government Information Quarterly* (31:1), pp. 119–128. (https://doi.org/10.1016/j.giq.2013.06.002).

Bason, C., and Austin, R. D. 2021. “Design in the Public Sector: Toward a Human Centred Model of Public Governance,” *Public Management Review*, Routledge, pp. 1–31. (https://doi.org/10.1080/14719037.2021.1919186).

Bekkers, V., and Homburg, V. 2007. “The Myths of E-Government: Looking Beyond the Assumptions of a New and Better Government,” *The Information Society* (23:5), pp. 373–382. (https://doi.org/10.1080/01972240701572913).

Bhargav-Spantzel, A., Camenisch, J., Gross, T., and Sommer, D. 2007. “User Centricity: A Taxonomy and Open Issues,” *Journal of Computer Security* (15:5), IOS Press, pp. 493–527. (https://doi.org/10.3233/JCS-2007-15502).

Boell, S., and Cecez-Kecmanovic, D. 2015. “On Being ‘Systematic’ in Literature Reviews in IS,” *Journal of Information Technology* (30). (https://doi.org/10.1057/jit.2014.26).

Bokayev, B., Davletbayeva, Z., Amirova, A., Rysbekova, Z., Torebekova, Z., and Jussupova, G. 2021. “Transforming E-Government in Kazakhstan: A Citizen-Centric Approach,” *Innovation Journal* (26:1), pp. 1–21.

Bonina, C. M., and Cordella, A. 2009. “Public Sector Reforms and the Notion of ‘Public Value’: Implications for EGovernment Deployment,” in *Proceedings of the 15th Americas Conference on Information Systems*, p. 10.

Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., and Cleven, A. 2015. “Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research,” *Communications of the Association for Information Systems* (37). (https://doi.org/10.17705/1CAIS.03709).

Carter, L., and Bélanger, F. 2005. “The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factors,” *Information Systems Journal* (15:1), pp. 5–25. (https://doi.org/10.1111/j.1365-2575.2005.00183.x).

Codagnone, C., Misuraca, G., Gineikyte, V., and Barcevicius, E. 2020. “Exploring Digital Government Transformation: A Literature Review,” in *ICEGOV 2020: 13th International Conference on Theory and Practice of Electronic Governance*, pp. 502–509. (https://doi.org/10.1145/3428502.3428578).

Cohen, J. 1960. “A Coefficient of Agreement for Nominal Scales,” *Educational and Psychological Measurement* (20:1), pp. 37–46. (https://doi.org/10.1177/001316446002000104).

Coombes, P., and Nicholson, J. 2013. “Business Models and Their Relationship with Marketing: A Systematic Literature Review,” *Industrial Marketing Management* (42:5), pp. 656–664. (https://doi.org/10.1016/j.indmarman.2013.05.005).

Cooper, T. L., Bryer, T. A., and Meek, J. W. 2006. “Citizen-Centered Collaborative Public Management,” *Public Administration Review* (66:s1), pp. 76–88. (https://doi.org/10.1111/j.1540-6210.2006.00668.x).

Degbelo, A., Granell, C., Trilles, S., Bhattacharya, D., Casteleyn, S., and Kray, C. 2016. “Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience,” *ISPRS International Journal of Geo-Information* (5:2). (https://doi.org/10.3390/ijgi5020016).

Deursen, A. J. A. M., and van Dijk, J. A. G. M. 2009. “Improving Digital Skills for the Use of Online Public Information and Services,” *Government Information Quarterly* (26:2), pp. 333–340. (https://doi.org/10.1016/j.giq.2008.11.002).

Deursen, A., van Dijk, J., and Ebbers, W. 2006. “Why E-Government Usage Lags Behind: Explaining the Gap Between Potential and Actual Usage of Electronic Public Services in the Netherlands,” in

Electronic Government, Lecture Notes in Computer Science, M. A. Wimmer, H. J. Scholl, Å. Grönlund, and K. V. Andersen (eds.), Berlin, Heidelberg: Springer, pp. 269–280. (https://doi.org/10.1007/11823100_24).

Dunleavy, P. 2005. "New Public Management Is Dead--Long Live Digital-Era Governance," *Journal of Public Administration Research and Theory* (16:3), pp. 467–494. (https://doi.org/10.1093/jopart/mui057).

Dwivedi, Y., Williams, M., Mitra, A., Niranjan, S., and Weerakkody, V. 2011. *Understanding Advances in Web Technologies: Evolution from Web 2.0 to Web 3.0*, presented at the 19th European Conference on Information Systems, ECIS 2011, January 1.

Eap, T. M., Hatala, M., and Gasevic, D. 2007. "Enabling User Control with Personal Identity Management," in *IEEE International Conference on Services Computing (SCC 2007)*, July, pp. 60–67. (https://doi.org/10.1109/SCC.2007.56).

Ebbers, W. E., Jansen, M. G. M., and van Deursen, A. J. A. M. 2016. "Impact of the Digital Divide on E-Government: Expanding from Channel Choice to Channel Usage," *Government Information Quarterly* (33:4), pp. 685–692. (https://doi.org/10.1016/j.giq.2016.08.007).

Ferlie, E., Ashburner, L., Fitzgerald, L., and Pettigrew, A. 1996. *The New Public Management in Action*, Oxford: Oxford University Press. (https://doi.org/10.1093/acprof:oso/9780198289029.001.0001).

Ferro, E., Helbig, N. C., and Gil-Garcia, J. R. 2011. "The Role of IT Literacy in Defining Digital Divide Policy Needs," *Government Information Quarterly* (28:1), pp. 3–10. (https://doi.org/10.1016/j.giq.2010.05.007).

Fountain, J. E. 2001. *Building the Virtual State Information Technology and Institutional Change*, Washington DC: Brookings Institution Press.

Fröhlich, K. 2017. "Evaluating the Effects of E-Government Initiatives on Citizen-Centric Goals at Selected Namibian Government Ministry," in *2017 IST-Africa Week Conference (IST-Africa)*, June 30, pp. 1–9. (https://doi.org/10.23919/ISTAFRICA.2017.8102361).

Gable, M. 2015. "Efficiency, Participation, and Quality: Three Dimensions of E-Government?," *Social Science Computer Review* (33:4), SAGE Publications Inc, pp. 519–532. (https://doi.org/10.1177/0894439314552390).

Ghosh Roy, S., and Upadhyay, P. 2017. "Does E-Readiness of Citizens Ensure Better Adoption of Government's Digital Initiatives? A Case Based Study," *Journal of Enterprise Information Management* (30:1), pp. 65–81. (https://doi.org/10.1108/JEIM-01-2016-0001).

Gjermundrød, H., and Dionysiou, I. 2015. "A Conceptual Framework for Configurable Privacy-Awareness in a Citizen-Centric EGovernment," *Electronic Government* (11:4), pp. 258–282. (https://doi.org/10.1504/EG.2015.071398).

Grimsley, M., and Meehan, A. 2007. "E-Government Information Systems: Evaluation-Led Design for Public Value and Client Trust," *European Journal of Information Systems* (16:2), pp. 134–148. (https://doi.org/10.1057/palgrave.ejis.3000674).

Gupta, K. P., Singh, S., and Bhaskar, P. 2018. "Citizens' Perceptions on Benefits of e-Governance Services," *International Journal of Electronic Governance* (10:1), pp. 24–55. (https://doi.org/10.1504/IJEG.2018.091261).

Hashim, K. F., Hashim, N. L., Ismail, S., Miniaoui, S., and Atalla, S. 2020. *Citizen Readiness to Adopt the New Emerging Technologies in Dubai Smart Government Services*, presented at the 2020 6th International Conference on Science in Information Technology: Embracing Industry 4.0: Towards Innovation in Disaster Management, ICSITech 2020, pp. 1–5. (https://doi.org/10.1109/ICSITech49800.2020.9392071).

Heeks, R. 2003. "Most EGovernment-for-Development Projects Fail: How Can Risks Be Reduced?," *IGovernment Working Paper No. 14*. (https://doi.org/10.2139/ssrn.3540052).

Helbig, N., Ramón Gil-García, J., and Ferro, E. 2009. "Understanding the Complexity of Electronic Government: Implications from the Digital Divide Literature," *Government Information Quarterly* (26:1), pp. 89–97. (https://doi.org/10.1016/j.giq.2008.05.004).

Hung, M. J. 2012. "Building Citizen-Centred E-Government in Taiwan: Problems and Prospects 1," *Australian Journal of Public Administration* (71:2), pp. 246–255. (https://doi.org/10.1111/j.1467-8500.2012.00764.x).

Iivari, J., and Iivari, N. 2011. “Varieties of User-Centredness: An Analysis of Four Systems Development Methods,” *Information Systems Journal* (21:2), Wiley Online Library, pp. 125–153.

Ingrams, A. 2019. “Public Values in the Age of Big Data: A Public Information Perspective,” *Policy and Internet* (11:2), pp. 128–148. (https://doi.org/10.1002/poi3.193).

Janssen, M., and Helbig, N. 2018. “Innovating and Changing the Policy-Cycle: Policy-Makers Be Prepared!,” *Platform Governance for Sustainable Development* (35:4, Supplement), pp. S99–S105. (https://doi.org/10.1016/j.giq.2015.11.009).

Jarke, J. 2021. “Co-Creating Digital Public Services,” in *Co-Creating Digital Public Services for an Ageing Society: Evidence for User-Centric Design*, Public Administration and Information Technology, J. Jarke (ed.), Cham: Springer International Publishing, pp. 15–52. (https://doi.org/10.1007/978-3-030-52873-7_3).

Jos, P. H., and Tompkins, M. E. 2009. “Keeping It Public: Defending Public Service Values in a Customer Service Age,” *Public Administration Review* (69:6), pp. 1077–1086. (https://doi.org/10.1111/j.1540-6210.2009.02065.x).

Karunasena, K., and Deng, H. 2011. “A Revised Framework For Evaluating The Public Value Of E-Government,” *Pacific Asia Conference on Information Systems (PACIS 2011 Proceedings)*, p. 13.

Kassen, M. 2021. “Understanding Decentralized Civic Engagement: Focus on Peer-to-Peer and Blockchain-Driven Perspectives on e-Participation,” *Technology in Society* (66), p. 101650. (https://doi.org/10.1016/j.techsoc.2021.101650).

Kitchenham, B. 2004. “Procedures for Performing Systematic Reviews,” *Keele, UK, Keele University* (33), pp. 1–26.

König, P. D. 2021. “Citizen-Centered Data Governance in the Smart City: From Ethics to Accountability,” *Sustainable Cities and Society* (75). (https://doi.org/10.1016/j.scs.2021.103308).

Kotamraju, N. P., and van der Geest, T. M. 2012. “The Tension between User-Centred Design and e-Government Services,” *Behaviour & Information Technology* (31:3), pp. 261–273. (https://doi.org/10.1080/0144929X.2011.563797).

Kumar, A. 2019. “Citizen-Centric Model of Governmental Entrepreneurship: Transforming Public Service Management for the Empowerment of Marginalized Women,” *Transforming Government: People, Process and Policy* (13:1), pp. 62–75. (https://doi.org/10.1108/TG-03-2018-0023).

Kurdi, H., Li, M., and Al-Raweshidy, H. S. 2010. “Taxonomy of Grid Systems,” in *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications*, IGI Global, pp. 20–43. (https://doi.org/10.4018/978-1-61520-686-5.ch002).

Kyakulumbye, S., Pather, S., and Jantjies, M. 2019. “Towards Design of Citizen Centric E-Government Projects in Developing Country Context: The Design-Reality Gap in Uganda,” *International Journal of Information Systems and Project Management* (7:4), pp. 55–73. (https://doi.org/10.12821/ijispm070403).

Larsson, K. K. 2021. “Digitization or Equality: When Government Automation Covers Some, but Not All Citizens,” *Government Information Quarterly* (38:1), p. 101547. (https://doi.org/10.1016/j.giq.2020.101547).

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., and Moher, D. 2009. “The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration,” *Journal of Clinical Epidemiology* (62:10), Elsevier, pp. e1–e34. (https://doi.org/10.1016/j.jclinepi.2009.06.006).

Mariën, I., and Prodnik, J. A. 2014. “Digital Inclusion and User (Dis)Empowerment: A Critical Perspective,” *Info* (16:6), pp. 35–47. (https://doi.org/10.1108/info-07-2014-0030).

Miles, M. B., Huberman, A. M., and Saldaña, J. 2014. *Qualitative Data Analysis: A Methods Sourcebook*, (Third edition.), Thousand Oaks, Califorinia: SAGE Publications, Inc.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., and for the PRISMA Group. 2009. “Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement,” *BMJ* (339:jul21 1), pp. b2535–b2535. (https://doi.org/10.1136/bmj.b2535).

Mossey, S., Manoharan, A. P., and Bennett, L. V. 2018. “Exploring Citizen- Centric E-Government Using a Democratic Theories Framework,” in *New Approaches, Methods, and Tools in Urban E-Planning*, pp. 1–32. (https://doi.org/10.4018/978-1-5225-5999-3.ch001).

Mostafa, M. M., and El-Masry, A. A. 2013. “Citizens as Consumers: Profiling e-Government Services’ Users in Egypt via Data Mining Techniques,” *International Journal of Information Management* (33:4), pp. 627–641. (https://doi.org/10.1016/j.ijinfomgt.2013.03.007).

Nabatchi, T. 2017. “Public Values Frames in Administration and Governance,” *Perspectives on Public Management and Governance* (1). (https://doi.org/10.1093/ppmgov/gvx009).

Norris, P., and Norris, M. L. in C. P. P. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge University Press.

OECD and Asian Development Bank. 2019. “Towards a Citizen-Centric Civil Service,” in *Government at a Glance Southeast Asia 2019*, OECD, pp. 19–35. (https://doi.org/10.1787/0f664ace-en).

Ølnes, S., Ubacht, J., Janssen, M. 2017. “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, ” *Government Information Quarterly* (34:3), pp. 355-364. (https://doi.org/10.1016/j.giq.2017.09.007).

Pang, M.-S., Lee, G., and DeLone, W. H. 2014. “IT Resources, Organizational Capabilities, and Value Creation in Public-Sector Organizations: A Public-Value Management Perspective,” *Journal of Information Technology* (29:3), pp. 187–205. (https://doi.org/10.1057/jit.2014.2).

Paré, G., Trudel, M.-C., Jaana, M., and Kitsiou, S. 2015. “Synthesizing Information Systems Knowledge: A Typology of Literature Reviews,” *Information & Management* (52:2), pp. 183–199. (https://doi.org/10.1016/j.im.2014.08.008).

Park, S., and Humphry, J. 2019. “Exclusion by Design: Intersections of Social, Digital and Data Exclusion,” *Information, Communication & Society* (22:7), Routledge, pp. 934–953. (https://doi.org/10.1080/1369118X.2019.1606266).

Parra, R. D., and Libaque-Saenz, C. 2020. *The Influence of Digital Transformation of the Peruvian Public Sector on Citizen Trust*, presented at the 26th Americas Conference on Information Systems, AMCIS 2020. (https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097714729&partnerID=40&md5=04e69671c7092986cb9bbc3782d8cf42).

Pérez-Morote, R., Pontones-Rosa, C., and Núñez-Chicharro, M. 2020. “The Effects of E-Government Evaluation, Trust and the Digital Divide in the Levels of e-Government Use in European Countries,” *Technological Forecasting and Social Change* (154), p. 119973. (https://doi.org/10.1016/j.techfore.2020.119973).

Pollitt, C., and Bouckaert, G. 2003. “Evaluating Public Management Reforms: An International Perspective,” in *Evaluation in Public-Sector Reform: Concepts and Practice in International Perspective*, Edward Elgar Publishing.

Purao, S., and Wu, A. 2013. *Towards Values-Inspired Design: The Case of Citizen-Centric Services*, in (Vol. 5), presented at the International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design, pp. 4427–4434. (https://www.scopus.com/inward/record.uri?eid=2-s2.0-84897753218&partnerID=40&md5=18fae709c0f905f6bf406edbfe4d505c).

Rein, M., and Schön, D. 1993. “Reframing Policy Discourse,” in *The Argumentative Turn in Policy Analysis and Planning*, F. Fischer and J. Forester (eds.), London: Duke University Press, pp. 145–166. (http://www.myilibrary.com?id=40672).

Robinson, J. P., Dimaggio, P., and Hargittai, E. 2003. “New Social Survey Perspectives on the Digital Divide,” *IT & Society* (1:5), p. 22.

Rodriguez, M. M., Casper, G., and Brennan, P. F. 2007. “Patient-Centered Design: The Potential of User-Centered Design in Personal Health Records,” *Journal of AHIMA* (78:4), American Health Information Management Association, pp. 44–46.

Rose, J., Persson, J. S., Heeager, L. T., and Irani, Z. 2015. “Managing E-Government: Value Positions and Relationships,” *Information Systems Journal* (25:5), pp. 531–571. (https://doi.org/10.1111/isj.12052).

Saldaña, J. 2013. *The Coding Manual for Qualitative Researchers*, (2nd ed.), Los Angeles: Sage Publications, Inc.

Scott, M., Delone, W., and Golden, W. 2016. "Measuring EGovernment Success: A Public Value Approach," *European Journal of Information Systems* (25:3), pp. 187–208. (https://doi.org/10.1057/ejis.2015.11).

Sevaldson, B. 2018. *Beyond User Centric Design*, presented at the Proceedings of RSD7, Relating Systems Thinking and Design 7, Turin, Italy, pp. 516–525. (https://rsdsymposium.org).

Sharma, R., Fantin, A.-R., Prabhu, N., Guan, C., and Dattakumar, A. 2016. "Digital Literacy and Knowledge Societies: A Grounded Theory Investigation of Sustainable Development," *The Promise and Reality: Assessing the Gap between Theory and Practice in ICT4D* (40:7), pp. 628–643. (https://doi.org/10.1016/j.telpol.2016.05.003).

Sorn-In, K., Tuamsuk, K., and Chaopanon, W. 2015. "Factors Affecting the Development of E-Government Using a Citizen-Centric Approach," *Journal of Science & Technology Policy Management*, Emerald Group Publishing Limited.

Spurlock, B., and O'Neil, J. 2009. "Designing an Employee-Centered Intranet and Measuring Its Impact on Employee Voice and Satisfaction," *Public Relations Journal* (3:2), pp. 1–20.

Stoker, G. 2006. "Public Value Management: A New Narrative for Networked Governance?," *American Review of Public Administration* (36:1), pp. 41–57. (https://doi.org/10.1177/0275074005282583).

Thomas, J. C. 2013. "Citizen, Customer, Partner: Rethinking the Place of the Public in Public Management," *Public Administration Review* (73:6), pp. 786–796. (https://doi.org/10.1111/puar.12109).

Van Velsen, L., van der Geest, T., ter Hedde, M., and Derks, W. 2009. "Requirements Engineering for E-Government Services: A Citizen-Centric Approach and Case Study," *Government Information Quarterly* (26:3), Elsevier, pp. 477–486.

Ventriss, C., Perry, J. L., Nabatchi, T., Milward, H. B., and Johnston, J. M. 2019. "Democracy, Public Administration, and Public Values in an Era of Estrangement," *Perspectives on Public Management and Governance* (2:4), pp. 275–282. (https://doi.org/10.1093/ppmgov/gvz013).

Van der Wal, Z., and van Hout, E. Th. J. 2009. "Is Public Value Pluralism Paramount? The Intrinsic Multiplicity and Hybridity of Public Values," *International Journal of Public Administration* (32:3–4), Routledge, pp. 220–231. (https://doi.org/10.1080/01900690902732681).

Wyatt, S. 1991. "Web of Welfare: The Social Security Office Gets Networked," *The Social Implications of the Operational Strategy*, Social Policy Series, pp. 21–30.

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

When public values and user-centricity in e-government collide – A systematic review

Linda Weigl [a,b,*], Tamara Roth [b,e], Alexandre Amard [b], Liudmila Zavolokina [c,d]

[a] Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands
[b] SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg City, Luxembourg
[c] Digital Society Initiative, University of Zurich, Zurich, Switzerland
[d] Department of Information Systems (DESI), HEC Lausanne, University of Lausanne, Lausanne, Switzerland
[e] Sam M. Walton College of Business, University of Arkansas, Fayetteville, United States of America

ARTICLE INFO

Keywords:
User-centricity
Citizen-centricity
Public values
E-government
Literature review

ABSTRACT

User-centricity in e-government is a double-edged sword. While it helps governments design digital services tailored to the needs of citizens, it may also increase the burden on users and deepen the digital divide. From an institutional perspective, these fundamental conflicts are inevitable. To better understand the role and effect of user-centricity in e-government, this paper analyses academic literature on user-centricity and public values. The analysis leads to three main insights: First, there is a conflict in citizen representation that may result from the normative dominance of decision-makers. Second, we identify an accountability conflict that can prevent user-centric innovation from thriving in a highly institutionalized environment. Third, we identify a pluralism conflict that emerges from a clash between the reality of a diverse society and the assumed homogeneity of actors. The need to address these conflicts increases with rapid technological innovation, such as distributed ledger technologies, artificial intelligence, and trust infrastructures. These technologies put the user at the center stage and permeate aspects of social life beyond government. In response to these insights, we outline suggestions for further research and practice.

1. Introduction

Public administrations worldwide embrace citizen-centricity as a key component of their organizational strategy (OECD & Asian Development Bank, 2019; Vesnic-Alujevic, Stoermer, Rudkin, Scapolo, & Kimbell, 2019). This new strategy also reflects governments' eagerness to explore new technologies that may help improve public services (Dwivedi, Williams, Mitra, Niranjan, & Weerakkody, 2011) and better incorporate the needs of citizens as users (Codagnone, Misuraca, Gineikyte, & Barcevicius, 2020; Sevaldson, 2018; Zavolokina, Sprenkamp, & Schenk, 2023). In e-government, the new focus on citizens as users has evolved into 'user-centricity'. This construct encompasses the involvement and participation of users in the *design* of digital public services applications – also referred to as *co-design* – and the adaption of digital systems to users' preferences at the *implementation* stage.

Despite their goal to improve the delivery of public services, some user-centric implementations assume an ambitious level of digital skills that not all users possess. A lack of these skills and relevant knowledge of underlying public procedures could, for instance, exclude citizens from the co-creation of digital public services in collaborative design approaches. The resulting intention-reality gap creates tensions that materialize in the so-called digital divide, i.e., a state in which significant portions of the population either lack the necessary digital skills or access to otherwise available technology (Robinson, Dimaggio, & Hargittai, 2003). Governments focused on user-centricity for their delivery of public services risk oppressing these already marginalized groups further by assuming a common level of digital skills and not accounting for socio-economic differences. At the same time, the implementation of user-centricity can be a powerful tool to empower citizens and better reflect their needs (Weigl, Amard, Marxen, Roth, & Zavolokina, 2022).

However, putting citizens' needs and expectations center stage is difficult and requires a holistic approach beyond mere revision of government processes. User-centric e-government affects the foundation of public service delivery and necessitates a careful balance between values

* Corresponding author.
E-mail addresses: l.weigl@uva.nl (L. Weigl), TRoth@walton.uark.edu (T. Roth), alexandre.amard@uni.lu (A. Amard), liudmila.zavolokina@dsi.uzh.ch (L. Zavolokina).

https://doi.org/10.1016/j.giq.2024.101956
Received 19 May 2023; Received in revised form 12 March 2024; Accepted 22 June 2024
Available online 28 June 2024

introduced by user-centricity and established public values. We define public value(s) in line with Moore (1995), who posits that the 'public value' encapsulates the shared expectations of citizens regarding government and public services. He argues that public organizations pursue public value to effectively address public needs. A common ground for all public value frames is that public values are often ambiguous, hybrid, contrasting, and overlapping (Stoker, 2006). That is, the support and fulfillment of values introduced or championed by user-centricity may clash with established public value frames. Resulting value conflicts are clear signs of value pluralism and require careful management of user-centric implementations (van der Wal & van Hout, 2009). Weigl et al. (2022), for instance, find that user-centricity is strongly aligned with values such as efficiency, innovation, transparency, or accountability to the public.

While these values reflect government institutions' general pursuit of legitimacy, reputation, and a democratic ethos, they introduce economic rationality, which is not typically at the core of public organizing (Mignerat & Rivard, 2015; Wiredu, 2012). To anticipate conflicts and best leverage the possibilities introduced by user-centricity, governments need to deepen their understanding of *how* user-centricity may align and conflict with established public values, and *what* causes these conflicts. Current studies either focus on general public value conflicts or the design of different approaches to user-centric digital services in e-government. Only few studies explore value conflicts between user-centric and public values in a digital government context (Weigl et al., 2022). The existing fragmented literature and often contradictory research results also do not elaborate on how potentially conflicting values can be reconciled in user-centric designs, projects, and initiatives. The consequences and sources of such value conflicts for e-government services are yet to be systematically analyzed (Ingrams, 2019).

Given the relevance of user-centric applications in e-government and the advancement of relevant technologies to facilitate such applications, the needs of service providers and recipients should be better integrated into user-centric designs. The resulting reconciliation of user-centricity with public values may support more inclusive services and inform the development of technologies for social good. Efforts to integrate user-centricity into public value frames include the identification of conflict areas and, most importantly, their sources. These efforts are relevant to avoid deviations from core public values post-implementation, which can carry an elevated risk of exacerbating societal disparities, eroding trust in governance, and compromising privacy. Moreover, without identifying the sources of conflicts between user-centricity and public values, those conflicts will be difficult to tackle or reduce.

Thus, our study aims to provide a systematic overview of the *status quo* on interactions between user-centricity and established public values. We identify value conflicts and their sources based on an abductive analysis of our data. These serve as the foundation for recommendations to support the integration of user-centric digital services with public values. We also outline future research directions at the intersection of public value theory and user-centricity in IS and digital government. Since our study intends to deliver a systematic overview and actionable recommendations on how emerging user-centric technologies across many levels of social organizing, such as digital identities and artificial intelligence (Ølnes, Ubacht, & Janssen, 2017), can be best integrated, we ask the following research questions:

RQ1. What value conflicts emerge in user-centric approaches to e-government?

RQ2. Why do these value conflicts between user-centric values and public values emerge?

To address these research questions, we first conduct a systematic literature review to synthesize literature in IS, management studies, and public administration. The synthesis helps us understand the interplay between user-centric and public values as well as emerging value conflicts. Based on abductive analyses, we explore underlying conflict sources, i.e., emerging or contextual factors that influence or exacerbate value conflicts. Second, we outline opportunities for further research to address the identified conflicts and assist the implementation of future user-centric government-to-citizen initiatives. Our study may also serve as a roadmap for user-centric approaches with new technological applications in e-government.

The remainder of the paper is structured as follows. The second section discusses the concepts of user-centricity and public policy, public values for e-government, and conflict literature. The third section outlines the research approach including literature identification, selection, relevance, quality assessment, data extraction and data analysis. The fourth section provides an overview of our findings. It describes the conflicts identified in our systematic literature review and integrates an analysis of their underlying sources. The fifth section discusses the research contributions and proposes areas for future research. The paper ends with a summary of our key findings, the paper's limitations, and an outline of future research directions.

2. Background

2.1. User-centricity and public policy

With the advent of digital transformation efforts at different governmental levels and the introduction of new technologies to improve public services, such as data analytics, AI, or novel identity management applications (Bhargav-Spantzel, Camenisch, Gross, & Sommer, 2006; Niglia & Tangi, 2024), user-centricity has become a primary goal for policy-makers (European Commission, 2023; OECD, 2009). While user-centric approaches were initially limited to human-computer interaction research in the 1980s, they have gained more widespread attention with the rise of software development projects. User-centric approaches commonly focus on user needs, expectations and preferences (Jarke, 2021; Kurdi, Li, & Al-Raweshidy, 2010). They also resonate well with software designers' X-centered designs, such as healthcare with patient-centered design (Morales Rodriguez, Casper, & Brennan, 2007), workplace with employee-centered design (Spurlock & O'Neil, 2009), or public administration with citizen-centric design (van Velsen, van der Geest, ter Hedde, & Derks, 2009a). Policy-makers and practitioners seized the advancement of user-centricity by developing national and international policies. For example, international organizations such as the OECD directly link user-centric digital public services to citizen well-being (Welby, 2019) and propose tailored guidance for the public (OECD, 2009). Extensive funding up to hundreds of millions of dollars[1] for projects targeting user-centricity further pushes these approaches. Many countries successfully embedded user-centricity in their service design, such as the U.S.A. (U. S. General Services Administration, 2023) and the U.K. (Government Digital Service, 2023). Some governments either directly support service designers aiming for user-centric designs or propose dedicated training (Government Digital Service, 2020). It is particularly relevant that service designers understand the importance of development and evaluation phases to achieve user-centric outcomes. IT develops rapidly, expecting citizens to catch up quickly. This is only possible when service designers can reflect different levels of digital skills and heterogenous needs in their applications to, for instance, accommodate an aging population (Lee, 2022).

The new focus on citizens as users may also affect policy-makers who need to consider the influences of user-centricity on policy-making and vice versa (Othman, Razali, & Nasrudin, 2020). Current considerations of this relationship have primarily focused on systems development. In this context, user-centricity appears as a multidimensional concept composed of four pillars (Iivari & Iivari, 2011): (1) user-centricity as user focus, (2) user-centricity as work-centeredness, (3) user-centricity as user involvement, and (4) user-centricity as system personalization.

[1] See, for instance, the projects listed on the website of the World Bank: https://projects.worldbank.org/en/projects-operations/project-detail/P168425

Each of these four pillars provides a different, albeit complementary, dimension to the concept. First, user focus addresses users' needs based on their activities or tasks and characteristics (such as skills or personal preferences). Second, work-centeredness provides insights into users' work activities, context, and dominant work practices. Third, user involvement reflects the importance and relevance users attach to a given system. Iivari and Iivari (2011) additionally distinguish between user involvement and user participation. The latter is a type of user involvement, in which users actively participate in the design process. Fourth, system personalization reflects the adaptability or adaptivity of the system's content structure, presentation, and functionalities to individual preferences or behaviors.

User-centric values steer how governments manage and integrate digital technologies into processes and interactions with citizens. However, the reconciliation between user-centric values in e-government and established public values has not been well-researched. Current work is focused on the benefits of user-centricity and primarily explores adoption mechanisms to overcome the challenges of e-government (Al-Hujran, Al-Debei, Chatfield, & Migdadu, 2015; Alzahrani, Al-Karaghouli, & Weerakkody, 2017; Rana, Williams, Dwivedi, & Williams, 2012; van Velsen et al., 2009a; Van Velsen, Van der Geest, Klaassen, & Steehouder, 2008), presenting user-centricity as a panacea. In practice, however, the proposed panacea has neither mitigated implementation struggles nor improved the acceptance of digital technologies in public administration.

The origin of user-centric approaches may explain their limited effect in practice. User-centricity is rooted in market-oriented principles, such as customer-centric relationships, and does not necessarily focus on users' 'true needs'. Instead, user-centricity considers, for instance, profit-maximizing strategies. This casts doubt on its representation of citizens' multifaceted needs and expectations and its contribution to social good in e-government contexts.

2.2. Public values for e-government

Maintaining or improving services and policies of system designs during digital transformation reflects the "inherently democratic mission [of public administration that] rely on support from citizens and institutions of government for their viability" (Ventriss, Perry, Nabatchi, Milward, & Johnston, 2019, p. 276). However, this mission is not necessarily reflected in the efficiency- and effectiveness-maximization principles of IS implementation (Mignerat & Rivard, 2015).

IS research typically adopts a rational perspective and considers managers as efficiency-seeking decision-makers, whose choices are based on cost-benefit analyses (Avgerou, 2000; Teo, Wei, & Benbasat, 2003; Tingling & Parent, 2002). Going beyond the ideal of a homo economicus in public administration (Avgerou, 2000; Orlikowski & Barley, 2001; Teo et al., 2003), would require actors to endorse public values as they seek legitimacy over efficiency (Jansen & Tranvik, 2011; Mignerat & Rivard, 2015). According to institutional theory, legitimacy is crucial for government actors to 'survive' long-term, that is, retain the support of their voters and be re-elected (Meyer & Rowan, 1977; Mignerat & Rivard, 2015).

Despite the clear focus on legitimacy in public administration, public management systems have changed over time and not all systems intrinsically prioritize 'public sector ethos' (Stoker, 2006). Traditional public administration, for instance, follows Weberian principles that position bureaucratic oversight as a central element to satisfying citizens' demands on the state (ibid.). The New Public Management (NPM) approach portrays citizens as 'customers' and heavily draws on private sector management models and market-based mechanisms (Ferlie, Ashburner, & Fitzgerald, 1996; Hood, 1995; Pollitt & Bouckaert, 2017). To achieve a more user-centric focus, Digital Era Governance (DEG) emerged as an attempt to re-aggregate public services around users' needs (Dunleavy, 2005). At the same time, the public value management paradigm (Stoker, 2006) highlights strategic objectives, such as enhancing efficiency in public services, ensuring equality, social inclusion, transparency, and upholding accountability (Cordella & Bonina, 2012; Moore, 1995). While these models and paradigms already try to anticipate values introduced by information technologies (IT), the complex relationship between ICT and citizen-centered governance warrants further analyses.

Bannister and Connolly (2014) have explored this intricate relationship by developing a typology of how technology implementation impacts a range of public values (Table 1). They refer to public values as "a mode of behavior [or] a way of doing things […] that is held to be right […] by the public, citizens or the so-called 'reasonable man'" (Bannister & Connolly, 2014, p. 120). This definition builds on 'public value' within the public value management paradigm and describes the shared expectations of citizens for government and public services (Moore, 1995). In their typology, Bannister and Connolly (2014) also identify several public values and categorize them into three domains: duty-oriented, service-oriented, and socially oriented. Duty-oriented values describe values related to the duties of the civil servant vis-à-vis the government. Service-oriented values reflect the responsibility of the civil servant to provide high-quality service to citizens as customers of public administration. Socially oriented values exhibit a broader set of social goods. The resulting typology can be mapped with other syntheses of public values in e-government. For instance, Rose, Persson, Heeager, and Irani (2015) highlight the ideals of professionalism, efficiency, service, and engagement. The ideal of professionalism builds on traditional bureaucratic values, also called 'foundational values' (Dobel, 2007), which are firmly established in democratic Western countries. Values of the professionalism ideal combine Bannister et al.'s (2014) socially and duty-oriented values. The efficiency ideal (Rose et al., 2015) draws on private sector management practice and shares similarities with industry-oriented and entrepreneurial governance approaches, such as NPM. It aims to encourage responsible spending of public resources and aligns with Bannister et al.'s (2014) service-oriented values. The service ideal follows a similar goal but takes a less market-oriented approach. Instead, it focuses on improving government services for citizens. Finally, the engagement ideal, which builds on Bannister et al.'s (2014) socially oriented values, highlights the involvement of citizens to strengthen a democratic approach to policy development.

Bannister et al.'s (2014) framework was updated as a result of

Table 1
Extended taxonomy of public values for user-centricity (based on Bannister & Connolly, 2014 and Weigl et al., 2022). * Marks the public values that we additionally identified in our systematic review.

Duty-oriented	Service-oriented	Socially oriented
Responsibility to the citizen / political neutrality* Compliance with the law Efficient use of public funds Facilitating the democratic will Accountability to government Economy of public funds Rectitude Legitimacy Representation of citizens' will and needs Sustainability*	Service to the citizen in his or her different roles Respect for the individual Responsiveness / proactivity* / flexible service delivery Effectiveness Efficiency Transparency Productivity Innovation	Inclusiveness Justice Fairness / equity* Equality of treatment and access Respect for the citizen Due process Protecting citizen privacy Protecting citizens from exploitation Protecting citizen security Accountability to the public Consultation / participation* / engagement* Impartiality Pluralism / diversity* Trust / confidence* / reliability*

changes to the government-citizens relationship through user-centric digitization (Weigl et al., 2022). The current study builds on a refined version of the extended public values typology by Weigl et al. (ibid.), specifically focusing on public values relevant for user-centricity in e-government projects.

2.3. Conflict literature

Public values, like the ones identified and catalogued by Bannister and Connolly (2014), are pervasive in public administration. Although largely invisible in daily practice, they shape the core of organizational behavior and routines. What is commonly referred to as organizational culture, comprises "a pattern or system of beliefs, values, and behavioral norms" (Schein, 2016, p. 88) that operate out of conscious awareness. They often materialize in the form of cultural artifacts like norms and practices (Leidner & Kayworth, 2006; Schein, 2016). As the organizational sociologist Lynne Zucker (1977) put it, "once institutionalized, [organizational culture] exists as a fact, as a part of objective reality" (p. 726). This renders organizational culture largely uncontested if not confronted with impulses from outside of the organizational context (Canato, Ravasi, & Phillips, 2013).

Organizational culture is particularly challenged in the context of public administration, where a push for more 'user democracy' and 'user-centricity' introduces change (de Graaf, Huberts, & Smulders, 2014) through processes adaptation and the adoption of IT (Sevaldson, 2018; van Velsen et al., 2009a). Many novel IT emphasize values conveyed by the concept of user-centricity, which often clash with established organizational values (de Graaf et al., 2014). Such conflicts between the adopted technology and organizational culture are commonly called cultural dissonance (Canato et al., 2013; Leidner & Kayworth, 2006).

However, value conflicts surrounding user-centricity do not only pertain to conflicts between IT-transferred/IT-inherent and organizational values. They can be a natural by-product of the value-laden exogenous political landscape (Aschhoff & Vogel, 2018; de Graaf et al., 2014). The resulting value pluralism leads to some values being championed over others, especially when values appear incompatible (Andersen, Jørgensen, Kjeldsen, Pedersen, & Vrangbæk, 2013; Spicer, 2001). Incompatibilities occur in connection with six central dimensions that are "neither […] superior to the other, nor are they equal in value" (Lukes, 1989, p. 125): (1) the purpose and role of government, (2) societal trends, (3) changing technologies, (4) information management, (5) human elements, and (6) interaction and complexity (Dawes, 2009, 2010). The first dimension focuses primarily on the definition of appropriate legal frameworks and performance evaluation methods to better distribute governmental responsibilities. Conflicts often occur between accountability, responsibility, transparency, stewardship, efficiency, effectiveness, and stakeholder values. The second conflict dimension involves demographic variables, such as economic background, ethnicity, and age, that greatly influence participation, the digital divide, and distributive social justice. Possibilities and risks tied to the implementation of novel IT characterize the third conflict dimension. The fourth dimension covers management issues ranging from quality assurance and the accuracy of information to accessibility and usability. The fifth conflict dimension elaborates on the human element, particularly the readiness for change and relevant skills. Finally, the sixth conflict dimension focuses on interaction and complexity, bringing together a cluster of elements that cross the technical, organizational, institutional and personal boundaries. 'Cross-boundary interactions', such as interoperability, collaboration, and cooperation, are particularly important because they rely on complex communication, management and governance dynamics (Dawes, 2009).

Value conflicts in public governance have already been researched extensively (Aschhoff & Vogel, 2018; Costa, Caldas, Coelho, & Gonçalves, 2016; de Graaf et al., 2014; Jørgensen & Bozeman, 2007; Nabatchi, 2017; Thacher & Rein, 2004; Ventriss et al., 2019). Yet, research often does not comprehensively address contradictions between established public values and IT-driven, emerging governance approaches like user-centricity. With increasing digitization of governments, this gap needs to be closed to avoid stalemates in public policy-making and to achieve normative consensus (Aschhoff and Vogel, 2018). More specifically, it is important to understand interactions between established democratic values and IT-based contemporary governance paradigms to establish feasible compromises. The relevance of this research becomes particularly apparent as new technologies, such as surveillance tools, blockchain, and AI, attract decision-makers' attention, and challenge established public values and democratic norms.

3. Research approach

To uncover dominant value conflicts between public values and values championed or introduced by user-centricity, and their conflict sources, we conduct a qualitative systematic literature review (Templier & Pare, 2018). This method helps us to systematically synthesize existing knowledge on public values in the context of user-centricity from different disciplines. At the same time, it enables us to understand the interplay between public values and prominent values of user-centricity. Since we primarily focus on academic literature, we may not capture current value conflicts that may have occurred in grey literature, industry reports, or case studies. Yet, many of our analyzed papers draw on practical examples so that we catch the most discussed value conflicts in e-government.

We follow a five-step systematic literature review approach focused on concepts as defined by Kitchenham (2004). We chose this concept-centric perspective over narrative, critical or realist approaches (Paré, Trudel, Jaana, & Kitsiou, 2015) to ensure replicability, rigor, and objectivity of the review process (Boell & Cecez-Kecmanovic, 2015). Concept-centricity also enabled us to focus specifically on public values in the context of user-centricity and not the overall public value discourse. Kitchenham (2004) describes five distinct steps: (1) study identification, (2) study selection, (3) study relevance and quality assessment, (4) data extraction, and (5) data synthesis. For step three, we used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol by Moher et al. (2009). Moreover, we included a snowball sampling step to saturate our data set to the best of our knowledge (Webster & Watson, 2002). The following subsections provide a more comprehensive overview of how we applied Kitchenham's (2004) five steps.

3.1. Study identification

We conducted a keyword search (see Table 2) across five databases (IEEE Xplore, ScienceDirect, SAGE Journals, SCOPUS, and Taylor and Francis). We used speech and spelling variants of our key concepts, such as "user-centricity", "user-centric", "user centric" and "user-centered", or "eGovernment" and "e-government" to avoid language bias. We also determined inclusion and exclusion criteria for our literature search according to discipline, topics, publication type, language and publication year (see Table 3).

As indicated in Table 3, we targeted publications from various disciplines. We avoided research on the early stages of e-government, which mainly explored the design of government portals and websites, by including only articles published in 2012 or later. We collected the initial data until February 2022. During the writing process of our paper, we conducted another data collection iteration to include recent publications. The last search was conducted in January 2023. See Tables 4-7 for further details and metadata, including the year of publication, publication type, method and geographic scope of the selected publications.

Table 2
Search strings for the systematic literature review.

#	Search String						
A	"User-centricity"	AND	"Government"	OR	"Public sector"	OR	"Public administration"
B	"Citizen-centricity"	AND	"Government"	OR	"Public sector"	OR	"Public administration"
C	"Values"	AND	"E-government"	OR	"Digital government"	OR	"Digital transformation"

Table 3
Literature search selection criteria. * Marks the criteria that had to be re-applied in the title and abstract selection procedure.

	Inclusion criteria	Exclusion criteria
Discipline*	Information Systems Library and Information Science Public Administration Economics and Sociology Public Policy Business, Management and Accounting Marketing and Sales	Engineering Computer Science and Security Mathematics Natural and Life Sciences
Topics*	User-centricity; citizen-centricity; e-government; emerging technologies; public values	Architecture; systems, government portals and websites; social media; survey studies from 2012 or before; value creation
Publication type	Book chapters Peer reviewed articles Doctoral theses Conference articles	Books Bachelor or Master theses
Language	English	Non-English
Publication year	2012 – 2023	Articles published before 2012

Table 4
Number of papers based on their publication year.

Year of publication	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Number of papers	6	11	7	8	9	3	7	6	4	8	1	1

Table 5
Number of papers based on their type.

Type of article	Book chapters	Conference articles	Peer-reviewed journal articles
Number of articles	5	16	50

Table 6
Number of papers based on the research method used.

Research method used	Design research	Formal	Mixed	Qualitative	Quantitative
Number of articles	3	2	7	44	15

3.2. Study selection

For the second step of Kitchenham's (2004) approach, we used the PRISMA protocol by Moher et al. (2009) in combination with the citation-chaining approach recommended by Webster and Watson (2002) (Fig. 1). PRISMA follows four steps – (1) identification, (2) screening, (3) eligibility, and (4) inclusion. During the identification stage, we collected 7168 potentially relevant scientific contributions after removing duplicates and books.[2] All identified literature was exported into the bibliographic reference manager Zotero. In the second phase, two authors independently screened the various papers based on a thorough assessment of their titles and narrowed the selection to 228 articles. The authors first presented their selection to each other and compared their results. After thorough discussion, only studies selected by both authors were considered for closer examination. During this exclusion procedure, we re-applied our pre-defined search selection criteria (Table 3).[3] In a sub-step of the screening phase, the two authors discussed selected publications based on their abstracts, which reduced the selection to 158 articles. In a further refinement exercise, we grouped the 158 articles according to the timeliness of their data and central foci (Kitchenham, 2004). After the exclusion of an additional 24 publications, we retained overall 134 articles. The excluded publications presented cases of digital transformation that we considered outdated or did not focus on technologies in the public sector. Examples include studies that analyzed social media, as well as studies with survey data from before 2012, or non-English publications. When retrieving full-text articles, eight papers were inaccessible, which reduced our number of studies to 126.

3.3. Study relevance and quality assessment

After reading the full papers, 47 out 126 articles were selected for our qualitative analysis. We selected these articles based on their relevance and usefulness in analyzing public values in the context of user-centricity. The quality of the papers is assessed through the articles' citations per year and the journal's impact factor. The snowball sampling added another 23 papers to our dataset. The update of our literature review in January 2023 yielded 1 paper that was not included in our literature search from the first cycle. This led to overall 71 papers eligible for qualitative analysis. The complete list of papers can be found in the Appendix.

Our selected papers are evenly distributed between 2012 and 2021. The data collection took place first in 2022 and later in 2023, which might explain the drop in analyzed articles from these 2 years.

50 papers were published in peer-reviewed journals, 16 in conference proceedings, and 5 in book chapters. This distribution highlights

[2] The search operators were usually applied to full text and metadata. However, in cases where our search yielded more than 700 publication results, we restricted the search fields to key words, abstract or introduction, depending on the available filters of each database.

[3] As the heterogenous search tools of the respective databases also yielded studies which were not related to our key concepts, we had to re-assess the selection criteria manually regarding the topic and discipline of the articles.

Table 7
Number of papers based on the origin of their data or focus of their analysis.

Data origin / analysis focus	Number of articles
Australia	1
Canada	2
Denmark	1
Egypt	1
Europe	3
Finland	3
France	1
Germany	3
Greece	1
Hong Kong	1
India	6
Iran	1
Jordan	1
Kazakhstan	1
Mexico	3
Namibia	1
Netherlands	3
New Zealand	1
Norway	1
Peru	1
Qatar	1
Rwanda	1
Singapore	1
Taiwan	1
Tanzania	1
Thailand	1
Turkey	1
UAE	1
Uganda	1
United Kingdom	1
United States	5
Worldwide	29

the overall high-quality of our selected papers.

Most articles were based on qualitative approaches, but 15 followed quantitative methods, and 7 used a mixed-method approach. Only 3 papers employed a design research method and 2 used formal methods.

Our selected papers covered a wide geographic range, with a satisfying mix of local, regional and worldwide foci. All continents were represented, which not only highlights the topic's relevance but also confirms our methodological rigor. For more details, the Table 7 provides a holistic summary. The number of papers, however, is not absolute since some studies had several countries as focal points. Where studies covered too many countries or were not specific enough, we listed them for the bigger geographical delimitation, i.e., Europe or worldwide.

3.4. *Data extraction*

We have already extracted the metadata from our literature while selecting studies using a spreadsheet. This helped us skim through titles and abstracts. Once the final set of literature was determined, the 71 downloaded articles were imported to MAXQDA, the software program used for our analysis (Mayring, 2014; Rädiker & Kuckartz, 2018).

3.5. *Data synthesis*

We performed a qualitative document analysis to synthesize and analyze our data. We manually coded 71 papers in two separate coding teams following a three-stage coding process (Fig. 2) of inductive and deductive coding (Saldaña, 2021). We began with open, inductive coding to identify general principles of user-centricity, which we define as first-order concepts (Gioia, Corley, & Hamilton, 2012) in our literature. In a second axial coding cycle, we coded deductively by referring back to the three user-centricity dimensions and the public value framework by Bannister and Connolly (2014). During this second coding process, we re-grouped and allocated, where possible, some of the codes from the first cycle into given dimensions and emerging frameworks, i.e., second-order themes (Gioia et al., 2012).

This process led to 5369 coded segments. To identify conflicts between public values and user-centricity as well as their context, we inductively re-analyzed the coded statements in a third cycle. During this third coding round, we summarized and aggregated our findings to identify the most salient conflict areas. The aggregation of our findings reduced the total number of coded segments to 5070 (Miles, Huberman, & Saldaña, 2014). In a repetition of the third cycle, we synthesized our set of codes by refining and reducing it to the most critical and useful concepts and categories. This cut the number of coded segments to 2504.

We performed a code relation analysis followed by a qualitative content analysis to identify the most dominant conflicts between user-centricity characteristics and public values (Mayring, 2014). The code

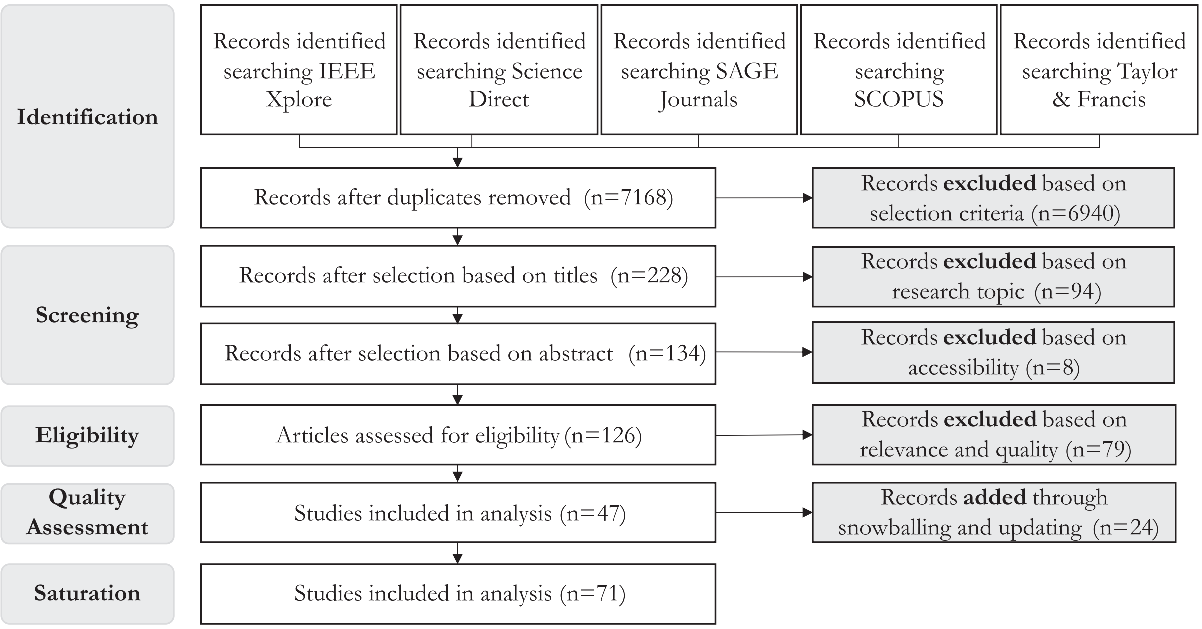

Identification
Records identified searching IEEE Xplore
Records identified searching Science Direct
Records identified searching SAGE Journals
Records identified searching SCOPUS
Records identified searching Taylor & Francis
Records after duplicates removed (n=7168)
Records **excluded** based on selection criteria (n=6940)
Screening
Records after selection based on titles (n=228)
Records **excluded** based on research topic (n=94)
Records after selection based on abstract (n=134)
Records **excluded** based on accessibility (n=8)
Eligibility
Articles assessed for eligibility (n=126)
Records **excluded** based on relevance and quality (n=79)
Quality Assessment
Studies included in analysis (n=47)
Records **added** through snowballing and updating (n=24)
Saturation
Studies included in analysis (n=71)

Fig. 1. Adapted PRISMA flow diagram (Kitchenham, 2004; Moher et al., 2009; Webster & Watson, 2002).

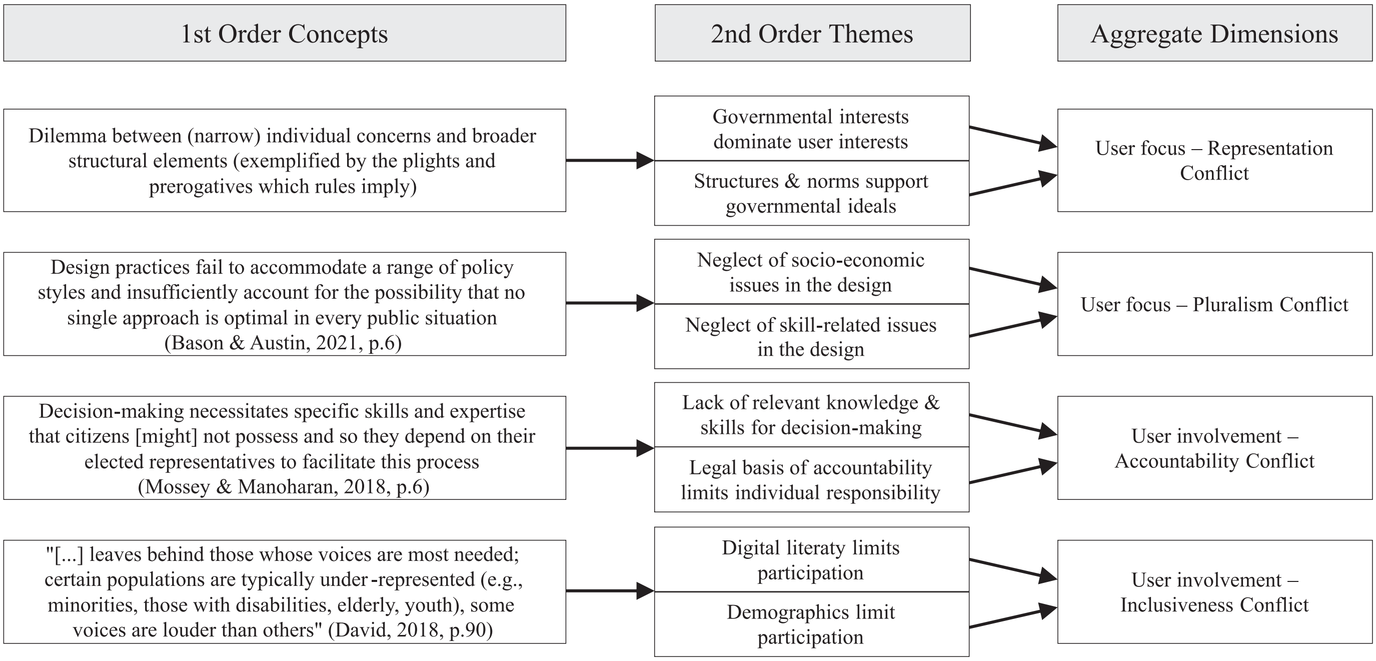

1st Order Concepts
2nd Order Themes
Aggregate Dimensions
Dilemma between (narrow) individual concerns and broader structural elements (exemplified by the plights and prerogatives which rules imply)
Governmental interests dominate user interests
Structures & norms support governmental ideals
User focus – Representation Conflict
Design practices fail to accommodate a range of policy styles and insufficiently account for the possibility that no single approach is optimal in every public situation (Bason & Austin, 2021, p.6)
Neglect of socio-economic issues in the design
Neglect of skill-related issues in the design
User focus – Pluralism Conflict
Decision-making necessitates specific skills and expertise that citizens [might] not possess and so they depend on their elected representatives to facilitate this process (Mossey & Manoharan, 2018, p.6)
Lack of relevant knowledge & skills for decision-making
Legal basis of accountability limits individual responsibility
User involvement – Accountability Conflict
"[...] leaves behind those whose voices are most needed; certain populations are typically under-represented (e.g., minorities, those with disabilities, elderly, youth), some voices are louder than others" (David, 2018, p.90)
Digital literacy limits participation
Demographics limit participation
User involvement – Inclusiveness Conflict

Fig. 2. Conflicts between public values in the context of user-centric e-government approaches.

relation analysis helped us observe co-occurrences in close proximity (in the same paragraph, for example) between codes that were assigned to one of the two main concepts. An additional qualitative coding query allowed us to investigate which co-occurrences indicate conflicts between established public values and values introduced or championed by user-centricity. Once we identified our main conflicts, two coders bilaterally discussed the allocated codes to contextualize dominant value conflicts.

This contextualization required a more abductive approach to identify concrete conflict sources as influencing factors. Abductive analysis typically “involves a recursive process of double-fitting data and theories” (Timmermans & Tavory, 2012, p. 179). That is, the author team met and discussed the coded segments that indicated a conflict source. We focused on recurring themes in different contexts across several of our analyzed papers. Our ‘revisiting of the phenomenon’ (Timmermans & Tavory, 2012) helped us discern the most salient conflict sources in our coded segments. Close observation of potential conflict sources also spurred ‘defamiliarization’, i.e., identifying “objects that were relegated to the background of our experience, as they were too taken for granted to be given a second thought” (Timmermans & Tavory, 2012, p. 177). Since many public values are a natural part of our status quo, they are difficult to identify even in a conflict situation. By deconstructing the status quo, we could alienate ourselves from the familiar and observe the causes of emerging conflict patterns. Our knowledge of relevant papers and theories in public administration, in addition to the occurrence of the same conflict sources across different cases, helped us to facilitate ‘alternate casing’ (Timmermans & Tavory, 2012) and discern our third-order codes. These codes delivered important insights underlying the emergence of conflicting values and user-centricity characteristics in e-government. We also repeatedly met to interpret the interplay between existing theories and their surfacing third-order codes. This included discussions about the differences and overlaps between our second-order themes and the aggregate dimensions (Gioia et al., 2012) until we reached an overall consensus.

4. Value conflicts and their causes

Our abductive coding helped us contextualize the dominant conflicts and identify the most plausible conflict sources by revisiting possible conflict sources in different contexts and actively deconstructing our own taken-for-granted status quo. This “iterative dialogue […] between data and an amalgam of existing and new conceptualizations” of value conflicts in e-government, allowed us to “cull […] and narrow […] possible theoretical leads” (Timmermans & Tavory, 2012, p. 180). More specifically, the revisiting of similar value conflicts and the defamiliarization of the public value context showed that not all identified conflicts in literature have their roots in values of user-centricity. It is rather the *implementation* of user-centric systems and services that introduces new and highlights specific public values over others. Alternate casing with different theories that pinpoint value deficiencies in either the user-centric system or the environment showed that the source of conflict is not the presence or absence of a certain public value, but value pluralism. Value pluralism occurs when several values are relevant but not equally prioritized. The simultaneous fulfillment of particular or multiple public values automatically (sometimes unintentionally) sacrifices or diminishes other non-negotiable public values, which leads to value conflicts. We specifically identified conflicts between established public values and values introduced or championed by user-centricity.

In this section, we elaborate on the abductive analysis of the value conflicts that have been identified between the user-centricity dimensions and public values in e-government. Since many user-centric values appear naturally aligned with values in public administration, many conflicts were unexpected. Overall, we found four dominant conflicts (see Table 8): (1) a user focus-representation conflict based on the assumption that citizens and governments have diverging interests and needs; (2) a user focus-pluralism conflict, which posits that users are not solely the target group of young, educated, and technology-conscious people; (3) a user involvement-accountability conflict that contrasts the compatibility of active citizen participation with the accountability of public officials; (4) a user involvement-inclusiveness conflict that illustrates the selective representation of citizens through digital channels. After identifying the four dominant conflicts from the literature, we wanted to better understand their context and identify potential causal links. Revisiting these conflicts and their sources provided the ground for a deeper, more nuanced discussion among the author team. During the subsequent defamiliarization phase, we aimed to find plausible explanations and sources from which the identified conflicts materialized by deconstructing the moral foundations of the

Table 8
Summary of value conflicts and conflict sources identified in the literature.

Value conflict	Conflict dynamic
User focus-representation	Citizens and governments have diverging interests and needs. Due to this divergence, governments cannot represent users' needs to the extent prescribed by user-centricity.
User focus-pluralism	The implementation of a user-centric technology can face the possibility that no single approach is optimal in every public situation in a pluralistic society that tolerates and supports diversity.
User involvement-accountability	Incompatibility between the active participation of citizens on the one hand, and the accountability of public officials at the government level on the other.
User involvement-inclusiveness	Inclusiveness in the collaborative design stage might be impaired due to citizens involvement through online channels and platforms.

Conflict source	Conflict source dynamic
Decision-making dominance	Pertains to the power imbalance between experienced decision-makers (facilitators, experts, community members) and other involved stakeholders, such as IT professionals and research consultants. In case of doubt, decision-makers can overrule suggestions and prioritize their desired values in the system's design choices. Consequentially, decision-makers can countermand findings from user research and/or user-centric design approaches.
Degree of participation	Pertains to the extent to which citizens can arguably be involved in collaborative design. Oftentimes, the diverging interests of different social groups cannot be equally respected in a consolidated system design. Thus, due to a lack of resources, individual citizens can only participate up to a certain degree. In other words, some voices are not heard because the people who would express them lack the resources, including knowledge and awareness, or their participation is not sufficiently effective.
Resource deficit	Refers to two main elements: (1) The lack of technical information and digital literacy among the providers or recipients of digitized public services in an information society that relies on continuous learning, and technological knowledge. (2) Lacking financial means to be able to acquire the necessary devices or access to a network in order to make use of a digital service, and non-existent infrastructure, which hampers connection and thereby access to public services provided through digital channels.
Establishment-innovation issue	Results from novelty-averse, hierarchical and bureaucratic structures, as well as budgetary constraints in the public sector, and the dynamic, risk tolerant and agile nature of innovation. Service providers governance structure and cultures are thus too slow and stiff to embrace the fast and iterative methods required for user-centricity
Multistakeholder issue	Stems from problems arising from multistakeholder governance in which many, possibly conflicting interests are incorporated in the dialogue, decision-making, design and implementation. Simply put, within a service provider organization, different groups have conflicting interests that must be accounted for. User-centric design is overlapping with co-design or participatory design. This does not only refer to the involvement of users, but also to the representation of different stakeholders, such as the government itself, consulting experts, and citizens. Therefore, governments face complexities when trying to integrate users into the design of digital services. The multistakeholder issue also involves risks undermining the participatory nature of the user-centric ideal due to public mind manipulation by lobby groups if such co-design processes are not overseen properly.

conflict environment. Moreover, we iterated our emerging conflict sources with existing theories in public administration. This alternate casing allowed for a more holistic analysis of the possible conflict sources and helped us add nuance while ensuring a relevant degree of generalization (Timmermans & Tavory, 2012). In total, five conflict sources emerged (see Table 8): (1) the decision-dominance issue that encumbers decision-making processes due to power and information asymmetries; (2) the degree of participation issue that raises the question how citizens can and want to participate in collaborative design; (3) the resource deficit issue that refers to knowledge, literacy, and financial gaps; (4) the establishment-innovation issue that contrasts established organizational structures in public administration with organizational flexibility needed enable technological innovation; (5) the multistakeholder issue emerges from the challenge of uniting various stakeholder interests from governmental, industry and civic sector at regional or national level.

Since our findings reported in relation to the co-occurrence of conflicts and conflict sources emerged during an abductive analysis, we cannot speak of statistical causation or correlation. Whenever we refer to some of these contextual factors as *conflict sources*, we intend to provide a theory (Timmermans & Tavory, 2012) for the identified conflicts from a qualitative abductive point of view.

Table 9 displays the level of co-occurrence between conflicts and their sources based on our systematic literature review and subsequent abductive analysis. A detailed list of articles at the intersection of these concepts can be found in the Appendix in Table 11.

4.1. User focus-representation conflict

The *user focus-representation conflict* describes the divergent interests and needs of citizens and governments that culminate in the governments' inability to represent users' needs compatible with principles of user-centricity (Berg, Lindholm, & Högväg, 2021; Clark, 2021; de Graaf et al., 2014; Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Kyakulumbye, Pather, & Jantjies, 2019; Miniaoui, Hashim, Atalla, Hashim, & Ismail, 2020; Mossey, Manoharan, & Bennett, 2018; Nabatchi, 2012; Park & Humphry, 2019; Sigwejo & Pather, 2016; Sorn-in, Tuamsuk, & Chaopanon, 2015). Central to this claim are three main issues.

Firstly, governments typically focus on accountability as defined by law or on "fulfilling […] requirements rather than trying to understand the needs of their users" (Kotamraju & van der Geest, 2012, p. 1; Kyakulumbye et al., 2019; Miniaoui et al., 2020; Sorn-in et al., 2015). The narrow definition of accountability binds them to specific legally defined standards, which can result in a "dilemma between […] individual concerns and broader structural elements (exemplified by the plights and prerogatives which rules imply)" (de Graaf et al., 2014, p. 17; Grube, 2013). This dilemma is particularly highlighted in implementations of user-centricity where infamously complex and inflexible bureaucratic procedures prove difficult to align with users' preferences, such as simplicity, efficiency and anonymity. Such misalignment with

Table 9
Co-occurrence between conflicts and their sources.

	Conflict			
Conflict source	User focus-representation	User focus-pluralism	User involvement-accountability	User involvement-inclusiveness
Decision-making Dominance	**High**	*None*	**High**	Low
Degree of Participation	Low	Low	Low	**High**
Resource Deficit	Low	**High**	Low	**High**
Establishment-Innovation	Low	**High**	**High**	Low
Multistakeholder	**High**	Low	Low	*None*

user needs appears to stand in the way of more user-centric e-governments that desire "serious, long-term committed relationships with their citizens and inhabitants. [U]sers, on the other hand, particularly when they are in information-seeking mode, want a quick foray into e-government" and consider complex processes and long wait times tedious (Kotamraju & van der Geest, 2012, p. 11). These conflicting visions of a productive citizen-government relationship encumber a further integration of user-centric values into the design of e-governments (ibid.).

Secondly, even in less bureaucratic structures, service designers are "generally unaware of how their values influence the ability to achieve desired values of public participation, such as legitimacy, justice, and effective administration" (Clark, 2021, p. 5; Ingrams, 2019; Kotamraju & van der Geest, 2012; Sorn-in et al., 2015). They typically "choose to downplay the normative element of e-government and […] design and develop services based on their ideal, rather than the actual relationship between governments and citizens. [This naturally] has adverse consequences for e-government's user-centricity and, ultimately, its adoption and use" (Kotamraju & van der Geest, 2012, p. 3). Socio-technical dynamics of technology adoption and integration into social systems and processes are particularly affected. They are typically "inscribed with the rules, values and interests of typically dominant groups" (Park & Humphry, 2019, p. 935).

Thirdly, it is difficult to ensure that the quality, validity and representation of such multidimensional public opinion and user-generated data is not contested (Berg et al., 2021, p. 232; Kassen, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018; Nabatchi, 2012; Park & Humphry, 2019). Dominant decision-making, i.e., "where the individual will [is] superseded by the collective will" (Grube, 2013, p. 2) is the underlying conflict source in observed *user focus-representation conflicts.* It appears to be rooted in the challenges arising from increasing multi-stakeholder dynamics of user-centricity implementation, and the negligence of minority opinions in user-centric e-government designs.

4.2. *User focus-pluralism conflict*

The second critical conflict is the so-called *user focus-pluralism conflict* (Aschhoff & Vogel, 2018; Bason & Austin, 2022; Berg et al., 2021; Bokayev et al., 2021; Brown, 2021; Cordella & Bonina, 2012; de Graaf et al., 2014; Gupta, Bhaskar, & Singh, 2016; Gupta, Singh, & Bhaskar, 2016; Gupta, Singh, & Bhaskar, 2018; Kotamraju & van der Geest, 2012; Larsson, 2020; Madan & Ashok, 2022; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019; Scott, DeLone, & Golden, 2016). Here, pluralism does not refer to classical pluralism in political decision-making theory but relates to a pluralistic society that tolerates and supports diversity. The strong focus on technology in user-centric e-government approaches may jeopardize pluralism if primarily young, educated, affluent, and technology-conscious people can use the system (Aschhoff & Vogel, 2018; Berg et al., 2021; Bokayev et al., 2021; Brown, 2021; de Graaf et al., 2014; Gupta et al., 2018; Kotamraju & van der Geest, 2012). Design practices without the conscious integration of pluralism and different policy styles would counter user-centric ideals to equally include all members of society (Bason & Austin, 2022, p. 6; Cordella & Bonina, 2012; Park & Humphry, 2019).

At the same time, it is recommended "not to design for a very specific nonrepresentative target group or task" (Kotamraju & van der Geest, 2012, p. 8) since such a narrow focus can be costly and inefficient even in user-centric designs. "Good practice demands that design […] supports […] the most commonly performed tasks or requests, for the largest or most important target groups" (Aschhoff & Vogel, 2018; Kotamraju & van der Geest, 2012, p. 8). Thus, "social challenges such as language barriers, low digital literacy, low user-friendliness of government websites, inability to access internet and lack of awareness in citizens" should be tackled before shifting to public service formats that are only available to a select few (Gupta, Singh, & Bhaskar, 2016, p. 162). Digitally less literate citizens, or people with restricted access to technological devices and connectivity cannot be passed over. Dismissing their needs is morally questionable and would "disproportionally affect citizens with low socio-economic status and demographic groups already suffering from other types of discrimination" (Gupta et al., 2018; Larsson, 2020, p. 2; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019).

The establishment-innovation issue and resource deficits explain the existence and saliency of this conflict in user-centric approaches (Aschhoff & Vogel, 2018; Bason & Austin, 2022; de Graaf et al., 2014; Grube, 2013). Different from private services, government services need to be relevant and available for all (Kotamraju & van der Geest, 2012). This is a complex endeavor and "runs counter to user-centricity" (ibid, p. 11). At the same time, governments cannot let their digital transformation be driven by market logic. Such logic would risk enforcing socio-economic discrimination and goes against public values of impartiality and equality. Kotamraju and van der Geest, (2012, p.8) describe the establishment-innovation issue by summarizing some of the key challenges in user-centered designs for e-government: (1) users and governments hold contradicting visions of a task, (2) governments cannot choose the audience to which their services should be tailored, (3) users and governments have different commitments to legal rules and regulations, while (4) both have different desires about the nature of their relationship. Governments typically strive for a long-term and proactive relationship with their citizens, while users prefer a transactional relationship with their public service providers.

4.3. *User involvement-accountability conflict*

In the *user involvement-accountability conflict*, literature questioned the compatibility between the active participation of citizens in digital services design as envisioned by user-centric e-government and the required accountability for public officials (Aschhoff & Vogel, 2018; Bason & Austin, 2022; Berg et al., 2021; de Graaf et al., 2014; Ghosh Roy & Upadhyay, 2017; Grube, 2013; Ingrams, 2019; König, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018). The ideal of user involvement, typically highlighted in the context of user-centricity, encompasses the "tradition of participatory democracy […], including […] user democracy, listening to public opinion, and dialogue" (Aschhoff & Vogel, 2018, p. 10). Professional accountability, or what Bannister and Connolly (2014) term 'accountability to government', entails the "compliance of public managers with professional standards and formal rules and regulations" (Aschhoff & Vogel, 2018, p. 10; Kotamraju & van der Geest, 2012). Even if forced into user-centric approaches, these values are difficult to reconcile and often result in two conflicts.

First, public servants must comply with a complex set of standards and rules that citizens are unaware of (Aschhoff & Vogel, 2018; de Graaf et al., 2014; Grube, 2013; Kotamraju & van der Geest, 2012). These standards and rules limit citizen involvement to areas that do not require tight regulation. Thus, "all […] proactiveness of citizens and end users may be of little use or even get nullified" where they would be legally accountable for their involvement (Ghosh Roy & Upadhyay, 2017, p. 76). Bason and Austin (2022) further contrast this *classical* 'accountability' approach, which values 'scientific-ness' and fair outcomes, with *human-centered* (here user-centered) approaches propagating user empowerment. They argue that human-centered designs fail to sufficiently account for several requirements of public sector design, such as capacity constraints, different policy styles, and the reality of policy mixes (Bason & Austin, 2022).

Secondly, representative theory suggests that "decision-making necessitates specific skills and expertise that citizens [might] not possess" (Berg et al., 2021; Grube, 2013; Mossey et al., 2018, p. 6). Despite the desirability of citizen participation in user-centric e-government designs, there are risks that strong user involvement may swing "the pendulum […] too far from the rightly criticized technocratic vision of a smart city" (König, 2021, p. 6).

Power dynamics between decision-makers and stakeholders may further exacerbate the *user involvement-accountability conflict*. Government officials can overrule external stakeholder decisions that would not comply with regulations to ensure fairness and avoid arbitrary rulings. Yet, this power dynamic already foreshadows the establishment-innovation conflict, in which governmental structures determine to what extent user-centricity can be reconciled with existing hierarchies.

4.4. User involvement-inclusiveness conflict

User-centricity foresees the involvement of citizens in the design stage primarily online, which compromises inclusivity (Berg et al., 2021; Clark, 2021; David, 2018; Kassen, 2021; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019), manifesting in a *user involvement-inclusiveness conflict*. Citizen involvement "often leaves behind those whose voices are most needed [as it] it takes time, patience, and resources [as well as specifically trained] administrators and decision makers […] to deal with citizens" (David, 2018, p. 90). For example, digitally less literate citizens may face neglect in participatory e-government initiatives (Kassen, 2021; König, 2021; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019). Yet, this conflict does not only unilaterally emerge from the physical, financial, educational, or other socio-economic obstacles and barriers citizens might encounter. A focus on user involvement can further "[affect] inclusiveness, since deliberation can be a demanding form of participation" (Berg et al., 2021, p. 233), and "might reinforce existing inequalities in political participation" (ibid.; König, 2021; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019).

The degree of participation in user-centric designs, therefore, has a strong influence on the *user involvement-inclusiveness conflict*. User involvement and citizen engagement are often "neither realistic nor necessary" even if digital channels were available for all (König, 2021, p. 6). Participating citizens typically have the relevant knowledge and skills to interact with government technology (Berg et al., 2021; Bokayev et al., 2021; David, 2018; Gupta et al., 2018; Gupta, Singh, & Bhaskar, 2016; Park & Humphry, 2019), and can access their network and financial resources (David, 2018). The latter also often coincides with the readiness to adopt new technologies and ownership of digital devices (Gupta et al., 2018; Larsson, 2020; Mariën & Amon Prodnik, 2014). These characteristics systematically exclude user groups whose voices are already underrepresented in current e-government approaches (David, 2018; Mariën & Amon Prodnik, 2014). As such, the dimension of the *user involvement-inclusiveness conflict* shares similarities with *the user focus-pluralism conflict*. Both conflicts exacerbate the marginalization of user groups either at the collaborative design or the application and implementation stage.

5. Discussion and opportunities for further research

Integrating user-centricity into e-government services is not only a popular design approach, but also a widely recognized and desired requirement (Kujala, 2003; van Velsen, van der Geest, ter Hedde, & Derks, 2009b). Our systematic review of the academic literature shows that values introduced or championed by user-centricity designs sometimes conflict with established public values. According to the reviewed and synthesized literature on user-centricity and public values from 2012 to 2023, value conflicts occur in different contexts. Current research shows that they can either be core dynamics of user-centricity, causing a clash between user-centric approaches and public values, or they can occur as a result of user-centric implementations. To further elaborate on why these conflicts arise, we identified conflict sources through an iterative process of abduction in the selected literature. While our analysis provides plausible theories, further research will be required to empirically determine conflict sources or contextual factors and provide mitigation strategies. A potential starting point for empirical research is Dawes' (2009, 2010) six central conflict dimensions. We present how the dimensions may interact in Fig. 3.

In the remainder of the section, we focus only on the most relevant contributions for research and the path forward to furthering our understanding of the dynamics at play. That is, we elaborate on decision-making dominance in the context of user representation (5.1.), and the difficulty of bridging the gap between established government structures and innovation based on user-centric ideals while upholding the principles of government accountability (5.2.). We also touch on the problem of resource deficits to highlight the need for inclusive participation in user-centric e-government (5.3.). Our research presents a first step in closing the gap of translating values introduced or championed by user-centricity into public policies and service designs.

5.1. Decision-making dominance and the representation conflict

The representation of citizens as users is challenging when institutional structures require decision-makers to prioritize certain preferences over others. This raises questions of how user-centric design can ensure that participation is more equally distributed and how government can integrate user-centric values into the delivery of services (Vigoda-Gadot, 2002). Most importantly, research should explore the establishment of normative pluralism and prevent adverse effects for representation through the implementation of user-centric designs. This may also entail investigating if institutional structures would allow for an increased user focus, and if such a focus would yield promised benefits. Due to the involvement of different actors, which challenges the balance between optimal representation and efficient decision-making, we see a substantial overlap with Dawes' (2009) *interaction and complexity dimension*. Moreover, considering the influence of governmental decision-making on this balance warrants a deeper analysis of Dawes' (2009) first dimension – *the purpose and role of government* – concerned with governmental responsibility. Other research has started shedding light on these dynamics and deserves further exploration in this context. For example, the extent to which competent civil society representatives can support the design process and counterbalance unilateral decision-making (Pozzebon, Cunha, & Coelho, 2016; Yang & Pandey, 2011), and their capacity to bring consensus, trustworthiness and legitimacy (OECD, 2022; Porumbescu, 2016).

5.2. Establishment-innovation issue and the accountability conflict

Embedding accountability conflicts in user-centric approaches with the establishment-innovation issue presents a continuation of existing public administration paradigms. Where the NPM approach adopted market logic and private sector management models, the DEG and public value management paradigm emphasize citizen engagement in digital government initiatives and advocate for public values beyond performance-based indicators (Bryson, Crosby, & Bloomberg, 2014). The latter two thus accommodate key values of user-centricity to a greater extent than NPM. Yet, the accountability conflict shows that it is difficult for such new values to thrive in a highly institutionalized environment. Despite efforts to encourage a more innovative and user-centric mindset in public administration, additional research will be required on how the relationship between citizens and public administrations in e-government can be designed. Drawing on Dawes' (2009) conflict dimensions, we see an overlap with four dimensions: (1) *role and purpose of government*, which encompasses the legal, administrative and bureaucratic processes of the public institutions and their accountability; (2) *changing technologies*, which centers around the implementation of novel IT in institutions and organizations; (3) *information management*, which concerns information quality, accessibility and usability as part of a functioning innovation process; and (4) *societal trends*, which highlights the demographics of society, such as socio-economic status, income, age or education.

Relevant research to better apprehend these complex dynamics includes Fung (2015), who highlights the difficulty for public officials or public service providers to take responsibility for user-driven design

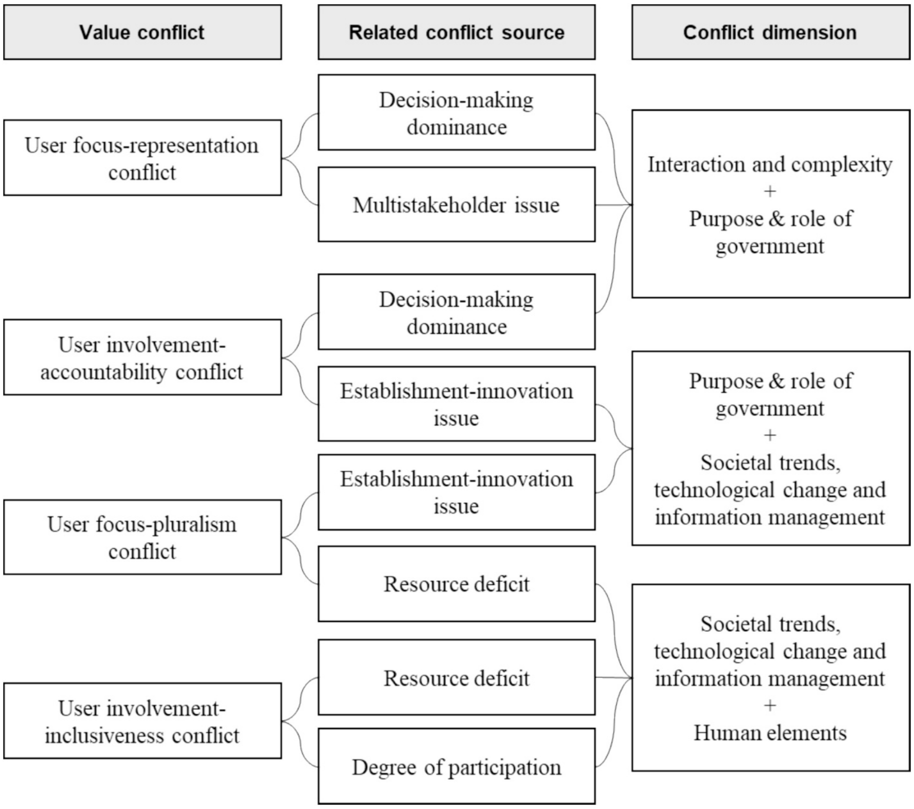

Value conflict
Related conflict source
Conflict dimension
User focus-representation conflict
Decision-making dominance
Multistakeholder issue
Interaction and complexity + Purpose & role of government
User involvement-accountability conflict
Decision-making dominance
Establishment-innovation issue
Purpose & role of government + Societal trends, technological change and information management
User focus-pluralism conflict
Establishment-innovation issue
Resource deficit
User involvement-inclusiveness conflict
Resource deficit
Degree of participation
Societal trends, technological change and information management + Human elements

Fig. 3. Embedding public value conflicts in user-centric e-government, their sources and Dawes' central conflict dimensions (2009, 2010).

choices – especially when users' preferences clash or are not reconcilable with established institutional rules and incentive systems. They suggest that policy-makers need to pay attention to the way they integrate user-centric IT into their interaction with citizens, and consider the "full menu of design choices" available to them (Fung, 2015; OECD, 2022). The role of specific agencies or ministerial branches – such as GovTech labs – that work at the intersection of public administration and industry has also been researched (Bharosa, 2022). In this context, their capacity to keep the balance between innovation and institutional norms has been highlighted. In fact, multidisciplinary teams encompassing innovative companies, academia and government, with a shared objective for innovating and the relevant budget to reach prototyping stages rapidly, have been suggested to support innovation without sacrificing governmental accountability (Tõnurist, Kattel, & Lember, 2017). Moreover, the integration of emerging innovations into value-sensitive design principles can ensure ethical alignment and user-centered development (Friedman & Hendry, 2019). This research angle deserves to be further explored so that adequate solutions can be found that strike a balance between fostering experimentation and ensuring responsible innovation.

5.3. *Resource deficit and the pluralism and inclusiveness conflict*

The conflict contrasts the reality of a diverse society with society's ideal of the digitally literate individual. The inclusiveness conflict with its focus on the pursuit of user engagement and the simultaneous discriminatory exclusion of individuals, is closely related (Mariën & Amon Prodnik, 2014). Both conflicts can be attributed to resource deficits, which encompass a lack of digital skills, a lack of financial resources, and insufficient access to digital infrastructure in rural areas. A lack of awareness among service designers, who are often unaware of inclusiveness challenges or do not know how to address them, can exacerbate the conflict (Bär, 2017). Yet, the much-needed involvement of citizens as stakeholders in the design process is often inhibited by the above-mentioned resource deficits.

Thus, a third path for future research is to analyze the impact of user-centricity on resource-based technological discrimination and exclusion, and on ways to mitigate these effects in practice. Continuing the work of Alomari, Sandhu, and Woods (2014) at a larger scale, the distinction of the impact in different geographical areas might be particularly interesting to evaluate. This would enable a more nuanced approach to account for different demographics and technological maturity across countries. Further research is also needed to better understand how government measures can impact individual resource deficits. It has been proposed, for instance, that developing digital literacy and digital skills alongside general educational objectives could present an effective measure (Choudhary & Bansal, 2022; Méndez-Domínguez, Carbonero Muñoz, Raya Díez, & Castillo De Mesa, 2023). It would require, for instance, the deployment of community officers to provide technology advice and support for digital public services (Suchowerska & McCosker, 2022), and investments into better affordability and coverage of digital public infrastructure (Shenglin, Simonelli, Ruidong, Bosc, & Wenwei, 2017). Research on the impact of non-digital alternatives as mitigation measures (see e.g., Reddick & Anthopoulos, 2014) also contributes to a better understanding of this challenge. This research can be grounded in four dimensions of Dawes' framework: (1) *changing technologies*; (2) *information management*; (3) *societal trends*; and (4) *human elements*.

6. Conclusion

User-centric principles in e-government garner support from different governments worldwide that seek to improve their public services. Aimed at benefitting the user, user-centricity is often assumed to naturally complement established public values. Governments typically build on public values to deliver services and interact with citizens. Our study challenges this assumption and deconstructs emerging conflicts between the implementation of values introduced or championed by user-centricity and established public values. We ground our analysis in a systematic literature review of user-centricity in e-government and gather evidence of value conflicts as well as their underlying sources. Our analysis included more than 7000 articles from an eleven-year period, out of which we qualitatively coded 71 in two separate coding teams. Following this extensive review, we synthesized the knowledge from three different disciplines and identified emerging patterns from individual observations.

We show that user-centricity and public values conflict in four notable areas: the conflict between *user focus* and citizen *representation* and *pluralism*, and the conflict between *user involvement* and government *accountability* and societal *inclusiveness*. Abductive reasoning helped us discern why these conflicts emerge. We postulate five main influencing factors: the *decision-making dominance issue*, the *degree of participation issue*, the *resource deficit issue*, the *establishment-innovation issue* and the *multistakeholder issue*. The prevalence of these issues within service delivery environments proves that they are not isolated or tangential. Instead, they pose a serious threat to user-centric e-government service provision success, which warrants further research in the following three areas: (1) the detection of other types of conflicts that were not found in the existing literature; (2) the evidence-based identification of causal relationships between prevalent issues in service delivery environments and these conflicts; and (3) the elaboration and testing of mitigating measures that can alleviate or remove the conflicts themselves, or their outcome.

Our proposed future research also hints at the main limitations of this study. We currently focus primarily on academic literature within particular disciplines and do not consider grey literature, industry reports, or case studies. This selection of specific criteria may bias our analysis. Moreover, expanding the range of sources for analysis could deliver results on emerging conflicts. These results may also support the establishment of causation between conflicts and issues beyond abduction. A more systematic approach to causation may also deliver insights into the nature of our influencing factors. That is, if they are conflict sources, aggravating factors, or have other types of influencing relationships. In addition, our research is limited with regard to deriving practical implications for the public, as the literature analysis focuses on synthesizing existing research rather than prescribing actions or policies. Finally, a systematic literature review is always tied to a predefined scope. While our research approaches the concept of user-centricity from a broad angle, thereby increasing the potential for generalization of our findings, it inevitably limits the potential to provide specific recommendations or instructions for practitioners to a specific problem, context, or technology.

CRediT authorship contribution statement

Linda Weigl: Writing – review & editing, Writing – original draft, Project administration, Methodology, Formal analysis, Data curation, Conceptualization. **Tamara Roth:** Conceptualization, Writing – review & editing, Writing – original draft, Formal analysis. **Alexandre Amard:** Conceptualization, Writing – original draft, Visualization, Formal analysis, Data curation. **Liudmila Zavolokina:** Conceptualization, Writing – original draft, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to extend their sincere gratitude to Hanna Marxen and Tom Barbereau for their review, insights, and encouragement on crystallizing their research into this manuscript, and their contribution to a conference publication outlining the preliminary results of this research project, upon which this manuscript builds.This research was funded by the Luxembourg National Research Fund (FNR) and PayPal PEARL (grant reference 13342933), as well as through the University of Zurich and the Digital Society Initiative under the DIZH postdoc fellowship of Liudmila Zavolokina. For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any author accepted manuscript version arising from this submission.

Appendix A. Appendix

Table 10
List of coded publications during the literature review process and their main characteristics.

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Conference article	2013	Abdellatif, Ahmed; Ben Amor, Nahla; Mellouli, Sehl	An intelligent framework for e-government personalized services	Proceedings of the 14th Annual International Conference on Digital Government Research	Worldwide	Design research
Peer-reviewed journal article	2012	Alomari, Mohammad; Woods, Peter; Sandhu, Kuldeep	Predictors for e-government adoption in Jordan: Deployment of an empirical evaluation based on a citizen-centric approach	Information Technology & People	Jordan	Quantitative
Peer-reviewed journal article	2013	Andersen, Lotte Bøgh; Jørgensen, Torben Beck; Kjeldsen, Anne Mette; Pedersen, Lene Holm; Vrangbæk, Karsten	Public Values and Public Service Motivation: Conceptual and Empirical Relationships	The American Review of Public Administration	Denmark	Quantitative
Peer-reviewed journal article	2018	Aschhoff, Nils; Vogel, Rick	Value conflicts in co-production: governing public values in multi-actor settings	International Journal of Public Sector Management	Germany	Qualitative
Peer-reviewed journal article	2022	Bason, Christian; Austin, Robert D.	Design in the public sector: Towards a human centred model of public governance	Public Management Review	Worldwide	Qualitative

(*continued on next page*)

Table 10 (*continued*)

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Peer-reviewed journal article	2021	Berg, Janne; Lindholm, Jenny; Högväg, Joachim	How do we know that it works? Designing a digital democratic innovation with the help of user-centered design	Information Polity	Finland	Quantitative
Conference article	2013	Berntzen, Lasse	Citizen-centric eGovernment Services	Proceedings of CENTRIC 2013: The Sixth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services	Europe	Quantitative
Peer-reviewed journal article	2021	Bokayev, Baurzhan; Davletbayeva, Zhuldyz; Amirova, Aigerim; Rysbekova, Zhanar; Torebekova, Zulfiya; Jussupova, Gul	Transforming *E*-government in Kazakhstan: A Citizen-Centric Approach	The Innovation Journal: The Public Sector Innovation Journal	Kazakhstan	Quantitative
Peer-reviewed journal article	2013	Borah, Sri Keshabananda	Implementation of citizen-centric e-Governance projects in Assam	IOSR Journal of Humanities and Social Science	India	Qualitative
Peer-reviewed journal article	2021	Brown, Prudence R.	Public Value Measurement vs. Public Value Creating Imagination – the Constraining Influence of Old and New Public Management Paradigms	International Journal of Public Administration	Worldwide	Qualitative
Peer-reviewed journal article	2014	Bryson, John M.; Crosby, Barbara C.; Bloomberg, Laura	Public Value Governance: Moving Beyond Traditional Public Administration and the New Public Management	Public Administration Review	USA	Qualitative
Peer-reviewed journal article	2021	Clark, Jill K.	Public Values and Public Participation: A Case of Collaborative Governance of a Planning Process	The American Review of Public Administration	USA	Qualitative
Peer-reviewed journal article	2014	Clarke, Amanda; Margetts, Helen	Governments and Citizens Getting to Know Each Other? Open, Closed, and Big Data in Public Management Reform: Open, Closed, and Big Data in Public Management Reform	Policy & Internet	Canada; United Kingdom; USA	Qualitative
Peer-reviewed journal article	2012	Cordella, Antonio; Bonina, Carla M.	A public value perspective for ICT enabled public sector reforms: A theoretical reflection	Government Information Quarterly	Worldwide	Qualitative
Book chapter	2018	David, Nina	Democratizing Government: What We Know About E-Government and Civic Engagement	International E-Government Development	Worldwide	Qualitative
Peer-reviewed journal article	2016	De Graaf, Gjalt; Huberts, Leo; Smulders, Remco	Coping With Public Value Conflicts	Administration & Society	Worldwide	Qualitative
Peer-reviewed journal article	2016	Degbelo, Auriol; Granell, Carlos; Trilles, Sergio; Bhattacharya, Devanjan; Casteleyn, Sven; Kray, Christian	Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience	ISPRS International Journal of Geo-Information	Worldwide	Qualitative
Conference article	2019	*E. Luna*, Dolores; Picazo-Vela, Sergio; Ramon Gil-Garcia, J.; Puron-Cid, Gabriel; Sandoval-Almazan, Rodrigo; F. Luna-Reyes, Luis	Public Value Creation through Digital Service Delivery from a Citizens' Perspective	Proceedings of the 20th Annual International Conference on Digital Government Research	Mexico	Qualitative
Peer-reviewed journal article	2016	Ebbers, Wolfgang E.; Jansen, Marloes G.M.; Van Deursen, Alexander J.A.M.	Impact of the digital divide on e-government: Expanding from channel choice to channel usage	Government Information Quarterly	Netherlands	Quantitative
Conference article	2017	Frohlich, Karin	Evaluating the effects of e-government initiatives on citizen-centric goals at selected Namibian Government Ministry	2017 IST-Africa Week Conference (IST-Africa)	Namibia	Qualitative
Peer-reviewed journal article	2015	Gable, Matt	Efficiency, Participation, and Quality: Three Dimensions of *E*-Government?	Social Science Computer Review	Worldwide	Qualitative
Conference article	2016	Garcia-Garcia, Luz Maria	User Centric e-Government: the Modernization of the National Institute of Migration at Mexico's Southern Border	Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance	Mexico	Qualitative
Conference article	2014	Garcia-Garcia, Luz Maria; Gil-Garcia, J. Ramon; Gómez, Victor	Citizen-centered e-government: towards a more integral approach	Proceedings of the 15th Annual International Conference on Digital Government Research	Worldwide	Qualitative

(*continued on next page*)

Table 10 (*continued*)

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Conference article	2015	Garcia-Garcia, Luz Maria; Gil-Garcia, J. Ramon; Gómez, Victor	Citizen centered e-government?: the case of National Migration Institute in the Southern Mexican border	Proceedings of the 16th Annual International Conference on Digital Government Research	Mexico	Qualitative
Peer-reviewed journal article	2017	Ghosh Roy, Saikat; Upadhyay, Parijat	Does e-readiness of citizens ensure better adoption of government's digital initiatives? A case based study	Journal of Enterprise Information Management	India	Mixed
Peer-reviewed journal article	2015	Gjermundrød, Harald; Dionysiou, Ioanna	A conceptual framework for configurable privacy-awareness in a citizen-centric eGovernment	Electronic Government, an International Journal	Worldwide	Design research
Peer-reviewed journal article	2013	Grube, Dennis	In Search of Society? The Limitations of Citizen-Centred Governance	The Political Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2016	Gupta, Kriti Priya; Bhaskar, Preeti; Singh, Swati	Critical Factors Influencing *E*-Government Adoption in India: An Investigation of the Citizens' Perspectives	Journal of Information Technology Research	India	Quantitative
Peer-reviewed journal article	2016	Gupta, Kriti Priya; Singh, Swati; Bhaskar, Preeti	Citizen adoption of e-government: a literature review and conceptual framework	Electronic Government, an International Journal	India	Mixed
Peer-reviewed journal article	2018	Gupta, Kriti Priya; Singh, Swati; Bhaskar, Preeti	Citizens' perceptions on benefits of e-governance services	International Journal of Electronic Governance	India	Quantitative
Conference article	2015	Haider, Muhammad; Khan, Muhammad Umer; Farooq, Sumbal	e-Government: An empirical analysis of current literature	2015 International Conference on Information and Communication Technologies (ICICT)	Worldwide	Qualitative
Conference article	2020	Hashim, Kamarul Faizal; Hashim, Nor Laily; Ismail, Solahudin; Miniaoui, Sami; Atalla, Shadi	Citizen Readiness to Adopt the New Emerging Technologies in Dubai Smart Government Services	2020 6th International Conference on Science in Information Technology (ICSITech)	UAE	Quantitative
Peer-reviewed journal article	2012	Hung, Mei Jen	Building Citizen-centred E-government in Taiwan: Problems and Prospects: Building Citizen-centred E-government in Taiwan	Australian Journal of Public Administration	Taiwan	Qualitative
Peer-reviewed journal article	2019	Ingrams, Alex	Public Values in the Age of Big Data: A Public Information Perspective: Public Values in the Age of Big Data	Policy & Internet	Germany; Netherlands	Qualitative
Peer-reviewed journal article	2018	Janssen, Marijn; Helbig, Natalie	Innovating and changing the policy-cycle: Policy-makers be prepared!	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2015	Jho, Whasun; Song, Kyong Jae	Institutional and technological determinants of civil e-Participation: Solo or duet?	Government Information Quarterly	Worldwide	Quantitative
Conference article	2013	Kamaruddin, Kamalia Azma; Noor, Nor Laila Md	Citizen-driven model in citizen-centric t-government	Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance	Worldwide	Qualitative
Peer-reviewed journal article	2021	Kassen, Maxat	Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation	Technology in Society	Finland; France; Germany	Qualitative
Peer-reviewed journal article	2021	König, Pascal D.	Citizen-centered data governance in the smart city: From ethics to accountability	Sustainable Cities and Society	Worldwide	Qualitative
Peer-reviewed journal article	2012	Kotamraju, Nalini P.; Van Der Geest, Thea M.	The tension between user-centred design and e-government services	Behavior & Information Technology	Netherlands	Qualitative
Peer-reviewed journal article	2019	Kumar, Avanish	Citizen-centric model of governmental entrepreneurship: Transforming public service management for the empowerment of marginalized women	Transforming Government: People, Process and Policy	India	Qualitative
Peer-reviewed journal article	2021	Kyakulumbye, Stephen; Pather, Shaun; Jantjies, Mmaki	Towards design of citizen centric e-government projects in developing country context: the design-reality gap in Uganda	International Journal of Information Systems and Project Management	Uganda	Qualitative

(*continued on next page*)

Table 10 (*continued*)

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Conference article	2015	Lappas, Georgios; Triantafillidou, Amalia; Kleftodimos, Alexandras; Yannas, Prodromos	Evaluation framework of local e-government and e-democracy: A citizens' perspective	2015 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)	Greece	Quantitative
Peer-reviewed journal article	2021	Larsson, Karl Kristian	Digitization or equality: When government automation covers some, but not all citizens	Government Information Quarterly	Norway	Qualitative
Conference article	2020	Liva, Giovanni; Codagnone, Cristiano; Misuraca, Gianluca; Gineikyte, Vaida; Barcevicius, Egidijus	Exploring digital government transformation: a literature review	Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance	Worldwide	Qualitative
Peer-reviewed journal article	2023	Madan, Rohit; Ashok, Mona	AI adoption and diffusion in public administration: A systematic literature review and future research agenda	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2014	Mariën, Ilse; A. Prodnik, Jernej	Digital inclusion and user (dis) empowerment: a critical perspective	Digital Policy, Regulation and Governance	Worldwide	Qualitative
Book chapter	2018	Mossey, Sean; Manoharan, A.P.; Bennett, Lamar Vernon	New Approaches, Methods, and Tools in Urban *E*-Planning	New Approaches, Methods, and Tools in Urban E-Planning:	USA	Mixed
Peer-reviewed journal article	2013	Mostafa, Mohamed M.; El-Masry, Ahmed A.	Citizens as consumers: Profiling e-government services' users in Egypt via data mining techniques	International Journal of Information Management	Egypt	Quantitative
Peer-reviewed journal article	2012	Nabatchi, Tina	Putting the "Public" Back in Public Values Research: Designing Participation to Identify and Respond to Values	Public Administration Review	Worldwide	Qualitative
Peer-reviewed journal article	2018	Nabatchi, Tina	Public Values Frames in Administration and Governance	Perspectives on Public Management and Governance	Worldwide	Qualitative
Book chapter	2018	Osborne, Stephen P.; Strokosch, Kirsty; Radnor, Zoe	Co-Production and the Co-Creation of Value in Public Services	Co-Production and Co-Creation	Worldwide	Qualitative
Peer-reviewed journal article	2014	Osman, Ibrahim H.; Anouze, Abdel Latef; Irani, Zahir; Al-Ayoubi, Baydaa; Lee, Habin; Balcı, Asım; Medeni, Tunç D.; Weerakkody, Vishanth	COBRA framework to evaluate e-government services: A citizen-centric perspective	Government Information Quarterly	Turkey	Mixed
Peer-reviewed journal article	2019	Panagiotopoulos, Panos; Klievink, Bram; Cordella, Antonio	Public value creation in digital government	Government Information Quarterly	Worldwide	Qualitative
Peer-reviewed journal article	2014	Pang, Min-Seok; Lee, Gwanhoo; DeLone, William H	IT Resources, Organizational Capabilities, and Value Creation in Public-Sector Organizations: A Public-Value Management Perspective	Journal of Information Technology	Worldwide	Qualitative
Peer-reviewed journal article	2019	Park, Sora; Humphry, Justine	Exclusion by design: intersections of social, digital and data exclusion	Information, Communication & Society	Australia	Qualitative
Conference article	2020	Parra, Raul Diaz; Saenz, Christian Fernando Libaque	The Influence of Digital Transformation of the Peruvian Public Sector on Citizen Trust	AMCIS 2020 Proceedings	Peru	Quantitative
Peer-reviewed journal article	2020	Pérez-Morote, Rosario; Pontones-Rosa, Carolina; Núñez-Chicharro, Montserrat	The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries	Technological Forecasting and Social Change	Europe	Quantitative
Peer-reviewed journal article	2013	Persaud, Ajax; Persaud, Priya	Rethinking *E*-Government Adoption: A User-Centered Model	International Journal of Electronic Government Research	Canada	Mixed
Book chapter	2013	Purao, Sandeep; Seng, Teo Chin; Wu, Alfred	Modeling Citizen-Centric Services in Smart Cities	Conceptual Modeling	Worldwide	Formal
Conference article	2013	Purao, Sandeep; Wu, Alfred	Towards Values-inspired Design: The Case of Citizen-Centric Services	Proceedings of the Thirty Fourth International Conference on Information Systems, Milan 2013	Worldwide	Formal
Peer-reviewed journal article	2015	Rose, Jeremy; Persson, John Stouby; Heeager, Lise Tordrup; Irani, Zahir	Managing e-Government: value positions and relationships	Information Systems Journal	Worldwide	Qualitative

(*continued on next page*)

Table 10 (*continued*)

Item Type	Publ. Year	Author	Title	Publication Title	Scope of analysis	Research type
Peer-reviewed journal article	2016	Scott, Murray; DeLone, William; Golden, William	Measuring eGovernment success: a public value approach	European Journal of Information Systems	USA	Quantitative
Peer-reviewed journal article	2019	Sepasgozar, Samad M.E.; Hawken, Scott; Sargolzaei, Sharifeh; Foroozanfa, Mona	Implementing citizen centric technology in developing smart cities: A model for predicting the acceptance of urban technologies	Technological Forecasting and Social Change	Iran	Mixed
Peer-reviewed journal article	2016	Sharma, Ravi; Fantin, Arul-Raj; Prabhu, Navin; Guan, Chong; Dattakumar, Ambica	Digital literacy and knowledge societies: A grounded theory investigation of sustainable development	Telecommunications Policy	Finland; Hong Kong; Qatar; New Zealand; Singapore	Qualitative
Peer-reviewed journal article	2016	Sigwejo, Annastellah; Pather, Shaun	A Citizen-Centric Framework For Assessing E-Government Effectiveness	The Electronic Journal of Information Systems in Developing Countries	Tanzania	Qualitative
Peer-reviewed journal article	2015	Sorn-in, Kanda; Tuamsuk, Kulthida; Chaopanon, Wasu	Factors affecting the development of e-government using a citizen-centric approach	Journal of Science & Technology Policy Management	Thailand	Mixed
Book chapter	2014	Synnes, Kåre; Kranz, Matthias; Rana, Juwel; Schelén, Olov; Nilsson, Michael	User-Centric Social Interaction for Digital Cities	Creating Personal, Social, and Urban Awareness through Pervasive Computing:	Worldwide	Qualitative
Peer-reviewed journal article	2013	Thomas, John Clayton	Citizen, Customer, Partner: Rethinking the Place of the Public in Public Management	Public Administration Review	Worldwide	Qualitative
Conference article	2012	Tsohou, Aggeliki; Lee, Habin; Irani, Zahir; Weerakkody, Vishanth; Osman, Ibrahim; Latif, Abdel Anuz; Medeni, Tunc	Evaluating e-government services from a citizens' perspective: a reference process	European, Mediterranean & Middle Eastern Conference on Information Systems 2012	Europe	Design research
Conference article	2017	Twizeyimana, Jean Damascene	User-centeredness and usability in e-government: a reflection on a case study in Rwanda	Proceedings of the Internationsl Conference on Electronic Governance and Open Society: Challenges in Eurasia	Rwanda	Qualitative

Table 11
Value conflicts and conflict sources found in literature.

	User focus-representation	User focus-pluralism	User involvement-accountability	User involvement-inclusiveness
Decision-making Dominance	Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Park & Humphry, 2019		de Graaf et al., 2014; Ingrams, 2019; Kotamraju & van der Geest, 2012; Mossey et al., 2018	David, 2018; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014
Degree of Participation	Berg et al., 2021; Grube, 2013; Kassen, 2021; Kotamraju & van der Geest, 2012; Nabatchi, 2012	Aschhoff & Vogel, 2018; Gupta, Singh, & Bhaskar, 2016; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014	Aschhoff & Vogel, 2018; Berg et al., 2021; de Graaf et al., 2014; König, 2021; Kotamraju & van der Geest, 2012; Mossey et al., 2018	David, 2018; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014
Resource Deficit	Kotamraju & van der Geest, 2012; Kyakulumbye et al., 2019; Sigwejo & Pather, 2016	Berg et al., 2021; Bokayev et al., 2021; Gupta et al., 2018; Gupta, Singh, & Bhaskar, 2016; Kotamraju & van der Geest, 2012; Larsson, 2020; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019	Kotamraju & van der Geest, 2012; Mossey et al., 2018	Berg et al., 2021; David, 2018; König, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014; Park & Humphry, 2019
Establishment-Innovation	de Graaf et al., 2014; Grube, 2013; Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Miniaoui et al., 2020	Aschhoff & Vogel, 2018; Brown, 2021; Cordella & Bonina, 2012; de Graaf et al., 2014; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014	Aschhoff & Vogel, 2018; Bason & Austin, 2022; de Graaf et al., 2014; Grube, 2013; Ingrams, 2019; Kotamraju & van der Geest, 2012; Mossey et al., 2018	Clark, 2021; Kotamraju & van der Geest, 2012; Mariën & Amon Prodnik, 2014
Multistakeholder	Ingrams, 2019; Kassen, 2021; Kotamraju & van der Geest, 2012; Nabatchi, 2012; Sorn-in et al., 2015	Aschhoff & Vogel, 2018; Kotamraju & van der Geest, 2012; Scott et al., 2016	Ingrams, 2019	

Table 12
Codebook.

Main code category	Sub-code category	Sub-code category
User-values conflict sources	Degree of participation	
	Multistakeholder issue	
	Establishment-innovation tension	
	Resource deficit	
	Decision-making dominance	
User-values overlap		
Knowledge society	ICT infrastructure	
	Role of new media	
	Regulatory policy and governance	
	Political vision	
	Human capital development	
	Education	
Facilitating conditions	Funding	
	Government process change	
	Coordination	
	Multichannel delivery of e-government	
	Access limitation	
	Infrastructure	
	Availability of data	
Collaborative governance	Influence	
	Citizen disinterest	
	Networks	
	Deliberation	
	Dialogue	
	Co-design	
Government	E-government	Policy-making
		Challenges, barriers and failures
		E-governance
		Infrastructure
		Success
		Risks
		Benefits
	Multiple Stakeholders	Coordination
		Interaction
		Dispute resolution
Design choices	Institutionalized processes	
	User-centered design	
	Value-infused design choices	
	Proactivity	
	Democracy	
	Inclusiveness	
	Performance	
	Productivity	
	Durability	
	Compliance	
	Engagement	
	Service quality	
	Efficiency	
	Political neutrality	
	Transparency	
	Trust	
	Accountability	Accountability to the public
		Accountability to government
	Cost savings	
	Equality	
	Responsiveness	
	Representation	
	Participation	
	Effectiveness	
	Justice	
	Legitimacy	
	Innovation	
	Equity	
	Confidence	
	Accessibility	
	Reliability	
	Fairness	
	Diversity	
	Flexibility	
	Sustainability	
	Economy / parsimony	
	Privacy	
	Security	
	Proper use of public funds	

(*continued on next page*)

Table 12 (*continued*)

Main code category	Sub-code category	Sub-code category
	Responsibility	
		Informed citizens
		Expected skills
	Skills	Awareness of existing system
		Knowledge
		Content availability and literacy
		Interoperability
Citizens	Needs	Needs, abilities and expectations
		Usability, functionality and accessibility
		Citizen satisfactions
		Ease of use
		Perceived usefulness
	Adoption	Citizen readiness
		Benefits
		Intention to use
Digital divide		
	System personalization	
User-centricity	User involvement	
	User focus	

References

Al-Hujran, O., Al-Debei, M., Chatfield, A., & Migdadu, M. (2015). The imperative of influencing citizen attitude toward e-government adoption and use. *Computers in Human Behavior, 53*, 189–203. https://doi.org/10.1016/j.chb.2015.06.025

Alomari, M. K., Sandhu, K., & Woods, P. (2014). Exploring citizen perceptions of barriers to e-government adoption in a developing country. *Transforming Government: People, Process and Policy, 8*(1), 131–150. https://doi.org/10.1108/TG-05-2013-0013

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review, 26*(1), 164–175. Scopus https://doi.org/10.1016/j.ibusrev.2016.06.004.

Andersen, L. B., Jørgensen, T. B., Kjeldsen, A. M., Pedersen, L. H., & Vrangbæk, K. (2013). Public values and public service motivation: Conceptual and empirical relationships. *The American Review of Public Administration, 43*(3), 292–311. https://doi.org/10.1177/0275074012440031

Aschhoff, N., & Vogel, R. (2018). Value conflicts in co-production: Governing public values in multi-actor settings. *International Journal of Public Sector Management, 31* (7), 775–793. https://doi.org/10.1108/IJPSM-08-2017-0222

Avgerou, C. (2000). Recognising alternative rationalities in the deployment of information systems. *The Electronic Journal of Information Systems in Developing Countries, 3*(1), 1–15. https://doi.org/10.1002/j.1681-4835.2000.tb00021.x

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly, 31*(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002

Bär, F. (2017). *Tackling knowledge gaps in digital service delivery*.

Bason, C., & Austin, R. D. (2022). Design in the public sector: Toward a human centred model of public governance. *Public Management Review, 24*(11), 1727–1757. https://doi.org/10.1080/14719037.2021.1919186

Berg, J., Lindholm, J., & Högväg, J. (2021). How do we know that it works? Designing a digital democratic innovation with the help of user-centered design. *Information Polity, 26*(3), 221–235. https://doi.org/10.3233/IP-200282

Bhargav-Spantzel, A., Camenisch, J., Gross, T., & Sommer, D. (2006). User centricity: A taxonomy and open issues. In *, 1–10. Proceedings of the Second ACM Workshop on Digital Identity Management*. https://doi.org/10.1145/1179529.1179531

Bharosa, N. (2022). The rise of GovTech: Trojan horse or blessing in disguise? A research agenda. *Government Information Quarterly, 39*, Article 101692. https://doi.org/10.1016/j.giq.2022.101692

Boell, S., & Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews in IS. *Journal of Information Technology, 30*. https://doi.org/10.1057/jit.2014.26

Bokayev, B., Davletbayeva, Z., Amirova, A., Rysbekova, Z., Torebekova, Z., & Jussupova, G. (2021). *Transforming E-government in Kazakhstan: A Citizen-Centric Approach. 26*.

Brown, P. R. (2021). Public value measurement vs. public value creating imagination – The constraining influence of old and new public management paradigms. *International Journal of Public Administration, 44*(10), 808–817. https://doi.org/10.1080/01900692.2021.1903498

Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2014). Public value governance: Moving beyond traditional public administration and the new public management. *Public Administration Review, 74*(4), 445–456. https://doi.org/10.1111/puar.12238

Canato, A., Ravasi, D., & Phillips, N. (2013). Coerced practice implementation in cases of low cultural fit: Cultural change and practice adaptation during the implementation of six sigma at 3M. *The Academy of Management Journal.*. https://doi.org/10.5465/amj.2011.0093

Choudhary, H., & Bansal, N. (2022). Addressing digital divide through digital literacy training programs: A systematic literature review. *Digital Education Review, 41*, 224–248. https://doi.org/10.1344/der.2022.41.224-248

Clark, J. K. (2021). Public values and public participation: A case of collaborative governance of a planning process. *The American Review of Public Administration, 51* (3), 199–212. https://doi.org/10.1177/0275074020956397

Codagnone, C., Misuraca, G., Gineikyte, V., & Barcevicius, E. (2020). Exploring digital government transformation: A literature review. In *ICEGOV 2020: 13th international conference on theory and practice of electronic governance* (pp. 502–509). Scopus. https://doi.org/10.1145/3428502.3428578.

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly, 29*(4), 512–520. https://doi.org/10.1016/j.giq.2012.03.004

Costa, A., Caldas, J. C., Coelho, R., de Ferreiro, M. F., & Gonçalves, V. (2016). The building of a dam: Value conflicts in public decision-making. *Environmental Values, 25*(2), 215–234. https://doi.org/10.3197/096327116X14552114338909

David, N. (2018). Democratizing government: What we know about E-government and civic engagement. In *International E-government development: Policy, implementation and best practice* (pp. 73–96). https://doi.org/10.1007/978-3-319-63284-1_4

Dawes, S. S. (2009). Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly, 26*(2), 257–264. https://doi.org/10.1016/j.giq.2008.12.003

Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly, 27*(4), 377–383. https://doi.org/10.1016/j.giq.2010.07.001

Dobel, J. P. (2007). Public management as ethics. In I. E. Ferlie, L. E. Lynn, & C. Pollitt (Eds.), *The Oxford handbook of public management* (pp. 156–181). Oxford University Press.

Dunleavy, P. (2005). New public management is dead—Long live digital-era governance. *Journal of Public Administration Research and Theory, 16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

Dwivedi, Y., Williams, M., Mitra, A., Niranjan, S., & Weerakkody, V. (2011). Understanding advances in web technologies: Evolution from WEB 2.0 to WEB 3.0. In *19th European Conference on Information Systems, ECIS 2011*.

European Commission. (2023). *eGovernment benchmark 2023 insight report—Connecting digital governments*. Publications Office of the European Union.

Ferlie, E., Ashburner, L., & Fitzgerald, L. (1996). *The new public Management in Action*. Oxford University Press.

Friedman, B., & Hendry, D. G. (2019). *Value sensitive design: Shaping technology with moral imagination*. MIT Press.

Fung, A. (2015). Putting the public Back into governance: The challenges of citizen participation and its future. *Public Administration Review, 75*(4), 513–522. https://doi.org/10.1111/puar.12361

Ghosh Roy, S., & Upadhyay, P. (2017). Does e-readiness of citizens ensure better adoption of government's digital initiatives? A case based study. *Journal of Enterprise Information Management, 30*, 65–81. https://doi.org/10.1108/JEIM-01-2016-0001

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Government Digital Service. (2020). *User-centred design: Training and events*. Gov: Uk. https://www.gov.uk/service-manual/design/user-centred-design-training-and-events.

Government Digital Service. (2023). *Design—Service manual*. Gov: Uk. https://www.gov.uk/service-manual/design.

de Graaf, G., Huberts, L., & Smulders, R. (2014). Coping with public value conflicts. *Administration and Society, 48*(9), 1101–1127. https://doi.org/10.1177/0095399714532273

Grube, D. (2013). In search of society? The limitations of citizen-Centred governance. *The Political Quarterly, 84*. https://doi.org/10.1111/j.1467-923X.2013.12024.x

Gupta, K., Bhaskar, P., & Singh, S. (2016). Critical factors influencing E-government adoption in India: An investigation of the citizens' perspectives. *Journal of*

Information Technology Research, 9, 28–44. https://doi.org/10.4018/JITR.2016100103

Gupta, K., Singh, S., & Bhaskar, P. (2016). Citizen adoption of e-government: A literature review and conceptual framework. *Electronic Government, an International Journal, 12*, 160. https://doi.org/10.1504/EG.2016.076134

Gupta, K., Singh, S., & Bhaskar, P. (2018). Citizens' perceptions on benefits of e-governance services. *International Journal of Electronic Governance, 10*, 24. https://doi.org/10.1504/IJEG.2018.091261

Hood, C. (1995). The "new public management" in the 1980s: Variations on a theme. *Accounting, Organizations and Society, 20*(2), 93–109. https://doi.org/10.1016/0361-3682(93)E0001-W

Iivari, J., & Iivari, N. (2011). Varieties of user-centredness: An analysis of four systems development methods. *Information Systems Journal, 21*(2), 125–153. https://doi.org/10.1111/j.1365-2575.2010.00351.x

Ingrams, A. (2019). Public values in the age of big data: A public information perspective. *Policy & Internet, 11*(2), 128–148. https://doi.org/10.1002/poi3.193

Jansen, A., & Tranvik, T. (2011). *The state of IT governance: Patterns of variation at the central government level in Norway* (p. 6846). https://doi.org/10.1007/978-3-642-22878-0_14

Jarke, J. (2021). Co-creating digital public services. In J. Jarke (Ed.), *Co-creating digital public Services for an Ageing Society: Evidence for user-centric design* (pp. 15–52). Springer International Publishing. https://doi.org/10.1007/978-3-030-52873-7_3.

Jørgensen, T. B., & Bozeman, B. (2007). Public values: An inventory. *Administration and Society, 39*(3). https://doi.org/10.1177/0095399707300

Kassen, M. (2021). Understanding decentralized civic engagement: Focus on peer-to-peer and blockchain-driven perspectives on e-participation. *Technology in Society, 66*, Article 101650. https://doi.org/10.1016/j.techsoc.2021.101650

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*, 1–26.

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society, 75*, Article 103308. https://doi.org/10.1016/j.scs.2021.103308

Kotamraju, N. P., & van der Geest, T. M. (2012). The tension between user-centred design and e-government services. *Behaviour & Information Technology, 31*(3), 261–273. https://doi.org/10.1080/0144929X.2011.563797

Kujala, S. (2003). User involvement: A review of the benefits and challenges. *Behaviour & Information Technology, 22*(1), 1–16. https://doi.org/10.1080/01449290301782

Kurdi, H., Li, M., & Al-Raweshidy, H. S. (2010). Taxonomy of grid systems. In *Handbook of research on P2P and grid Systems for Service-Oriented Computing: Models, methodologies and applications* (pp. 20–43). IGI Global. https://doi.org/10.4018/978-1-61520-686-5.ch002.

Kyakulumbye, S., Pather, S., & Jantjies, M. (2019). *Towards design of citizen centric e-government projects in developing country context: The design-reality gap in Uganda* (pp. 55–73). https://doi.org/10.12821/ijispm070403

Larsson, K. (2020). Digitization or equality: When government automation covers some, but not all citizens. *Government Information Quarterly, 38*, Article 101547. https://doi.org/10.1016/j.giq.2020.101547

Lee, C. (2022). Technology and aging: The jigsaw puzzle of design, development and distribution. *Nature Aging, 2*(12). https://doi.org/10.1038/s43587-022-00325-6. Article 12.

Leidner, D., & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30*, 357–399. https://doi.org/10.2307/25148735

Lukes, S. (1989). Making sense of moral conflict. In N. L. Rosenblum (Ed.), *Liberalism and the moral life* (pp. 127–142).

Madan, R., & Ashok, M. (2022). AI adoption and diffusion in public administration: A systematic literature review and future research agenda. *Government Information Quarterly, 40*. https://doi.org/10.1016/j.giq.2022.101774

Mariën, I., & Amon Prodnik, J. (2014). Digital inclusion and user (dis)empowerment: A critical perspective. *Info, 16*, 35–47. https://doi.org/10.1108/info-07-2014-0030

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation*. Open Access Repository: Basic Procedures and Software Solution.

Méndez-Domínguez, P., Carbonero Muñoz, D., Raya Díez, E., & Castillo De Mesa, J. (2023). Digital inclusion for social inclusion. Case study on digital literacy. *Frontiers in Communication, 8*. https://doi.org/10.3389/fcomm.2023.1191995

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550

Mignerat, M., & Rivard, S. (2015). Positioning the institutional perspective in information systems research. In L. P. Willcocks, C. Sauer, & M. C. Lacity (Eds.)*, Vol. 2. Formulating research methods for information systems* (pp. 79–126). Palgrave Macmillan UK. https://doi.org/10.1057/9781137509888_4.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications, Inc.

Miniaoui, S., Hashim, K., Atalla, S., Hashim, N. L., & Ismail, S. (2020). *Citizen Readiness to Adopt the New Emerging Technologies in Dubai Smart Government Services*. https://doi.org/10.1109/ICSITech49800.2020.9392071

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & for the PRISMA Group. (2009). *Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement*. https://doi.org/10.1136/bmj.b2535

Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.

Morales Rodriguez, M., Casper, G., & Brennan, P. F. (2007). Patient-centered design. The potential of user-centered design in personal health records. *Journal of AHIMA, 78* (4), 44–46. quiz 49–50.

Mossey, S., Manoharan, A., & Bennett, L. (2018). *Exploring citizen-centric E-government using a democratic theories framework* (pp. 1–32). https://doi.org/10.4018/978-1-5225-5999-3.ch001

Nabatchi, T. (2012). Putting the "public" Back in public values research: Designing participation to identify and respond to values. *Public Administration Review, 72*(5), 699–708. https://doi.org/10.1111/j.1540-6210.2012.02544.x

Nabatchi, T. (2017). Public values frames in administration and governance. *Perspectives on Public Management and Governance, 1*. https://doi.org/10.1093/ppmgov/gvx009

Niglia, F., & Tangi, L. (2024). Measuring user-centricity in AI-enabled European public services: A proposal for enabling maturity models. In *Research handbook on public management and artificial intelligence* (pp. 97–117). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781802207347/book-part-9781802207347-15.xml.

OECD. (2009). *Rethinking e-government services: User-Centred approaches*. Organisation for Economic Co-operation and Development. https://www.oecd-ilibrary.org/governance/rethinking-e-government-services_9789264059412-en.

OECD. (2022). OECD Guidelines for citizen participation processes. https://www.oecd.org/gov/oecd-guidelines-for-citizen-participation-processes-highlights.pdf.

OECD & Asian Development Bank. (2019). *Government at a glance Southeast Asia 2019*. OECD. https://doi.org/10.1787/9789264305915-en

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Orlikowski, W. J., & Barley, S. R. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? *MIS Quarterly, 25*(2), 145–165. https://doi.org/10.2307/3250927

Othman, M. H., Razali, R., & Nasrudin, M. (2020). *Key factors for E-government towards sustainable development goals. 29* pp. 2864–2876).

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Park, S., & Humphry, J. (2019). Exclusion by design: Intersections of social, digital and data exclusion. *Information, Communication & Society, 22*(7), 934–953. https://doi.org/10.1080/1369118X.2019.1606266

Pollitt, C., & Bouckaert, G. (2017). *Public management reform: A comparative analysis - into the age of austerity*. Oxford University Press.

Porumbescu, G. A. (2016). Linking public sector social media and e-government website use to trust in government. *Government Information Quarterly, 33*(2), 291–304. https://doi.org/10.1016/j.giq.2016.04.006

Pozzebon, M., Cunha, M. A., & Coelho, T. R. (2016). Making sense to decreasing citizen eParticipation through a social representation lens. *Information and Organization, 26* (3), 84–99. https://doi.org/10.1016/j.infoandorg.2016.07.002

Rädiker, S., & Kuckartz, U. (2018). *Analyse qualitativer Daten mit MAXQDA: Text, audio und video* (1. Aufl. 2019 ed.). Springer VS.

Rana, Williams, Dwivedi, & Williams. (2012). Theories and theoretical models for examining the adoption of E-government services. *E-Service Journal, 8*(2), 26. https://doi.org/10.2979/eservicej.8.2.26

Reddick, C., & Anthopoulos, L. (2014). Interactions with e-government, new digital media and traditional channel choices: Citizen-initiated factors. *Transforming Government: People, Process and Policy, 8*(3), 398–419. Scopus https://doi.org/10.1108/TG-01-2014-0001.

Robinson, J. P., Dimaggio, P., & Hargittai, E. (2003). New social survey perspectives on the digital divide. *IT & Society, 1*(5), 22.

Rose, J., Persson, J. S., Heeager, L. T., & Irani, Z. (2015). Managing e-government: Value positions and relationships. *Information Systems Journal, 25*(5), 531–571. https://doi.org/10.1111/isj.12052

Saldaña, J. (2021). The coding manual for qualitative researchers. *The Coding Manual for Qualitative Researchers.*, 1–440.

Schein, E. H. (2016). *Organizational culture and leadership* (5th ed.). Wiley (5. edition).

Scott, M., DeLone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems, 25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Sevaldson, B. (2018). Beyond user-centric design. In *Relating systems thinking and design symposium*. https://rsdsymposium.org/beyond-user-centric-design/.

Shenglin, B., Simonelli, F., Ruidong, Z., Bosc, R., & Wenwei, L. (2017). Digital infrastructure: Overcoming digital divide in emerging economies. https://pdfs.semanticscholar.org/a513/de546a8c8ceda79fb4e8492c15cd84c7f983.pdf.

Sigwejo, A., & Pather, S. (2016). A citizen-centric framework for assessing E-government effectiveness. *Electronic Journal of Information Systems in Developing Countries, 74*(1), 1–27. https://doi.org/10.1002/j.1681-4835.2016.tb00542.x

Sorn-in, K., Tuamsuk, K., & Chaopanon, W. (2015). Factors affecting the development of e-government using a citizen-centric approach. *Journal of Science and Technology Policy Management, 6*, 206–222. https://doi.org/10.1108/JSTPM-05-2014-0027

Spicer, M. W. (2001). Value pluralism and its implications for American public administration. *Administrative Theory & Praxis, 23*(4), 507–528.

Spurlock, B., & O'Neil, J. (2009). Designing an employee-centered intranet and measuring its impact on employee voice and satisfaction. *The Public Relations Journal, 3*(2), 1–20.

Stoker, G. (2006). Public value management: A new narrative for networked governance? *The American Review of Public Administration, 36*(1). https://doi.org/10.1177/0275074005282583. Article 1.

Suchowerska, R., & McCosker, A. (2022). Governance networks that strengthen older adults' digital inclusion: The challenges of metagovernance. *Government Information Quarterly, 39*(1), Article 101649. https://doi.org/10.1016/j.giq.2021.101649

Templier, M., & Pare, G. (2018). Transparency in literature reviews: An assessment of reporting practices across review types and genres in top IS journals. *European*

Journal of Information Systems, 27, 503–550. https://doi.org/10.1080/0960085X.2017.1398880

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt Interorganizational linkages: An institutional perspective. *MIS Quarterly, 27*(1), 19–49. https://doi.org/10.2307/30036518

Thacher, D., & Rein, M. (2004). Managing value conflict in public policy. *Governance: An International Journal of Policy, Administration and Institutions, 17*(4). https://doi.org/10.1111/j.0952-1895.2004.00254.x

Timmermans, S., & Tavory, I. (2012). Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological Theory, 30*(3).

Tingling, P., & Parent, M. (2002). Mimetic isomorphism and TechnologyEvaluation: Does imitation TranscendJudgment? *Journal of the Association for Information Systems, 3* (1). https://doi.org/10.17705/1jais.00025

Tõnurist, P., Kattel, R., & Lember, V. (2017). Innovation labs in the public sector: What they are and what they do? *Public Management Review, 19*. https://doi.org/10.1080/14719037.2017.1287939

U. S. General Services Administration. (2023). *A collection of tools to bring human-centered design into your project* (p. 18F). https://methods.18f.govhttps://methods.18f.gov/.

Van Velsen, L., Van der Geest, T., Klaassen, R., & Steehouder, M. (2008). User-centered evaluation of adaptive and adaptable systems: A literature review. *The Knowledge Engineering Review, 23*(3), 261–281.

van Velsen, L., van der Geest, T., ter Hedde, M., & Derks, W. (2009a). Requirements engineering for e-government services: A citizen-centric approach and case study. *Government Information Quarterly, 26*(3), 477–486. https://doi.org/10.1016/j.giq.2009.02.007

van Velsen, L., van der Geest, T., ter Hedde, M., & Derks, W. (2009b). Requirements engineering for e-government services: A citizen-centric approach and case study. *Government Information Quarterly, 26*(3), 477–486. https://doi.org/10.1016/j.giq.2009.02.007

Ventriss, C., Perry, J. L., Nabatchi, T., Milward, H. B., & Johnston, J. M. (2019). Democracy, public administration, and public values in an era of estrangement. *Perspectives on Public Management and Governance, 2*(4), 275–282. https://doi.org/10.1093/ppmgov/gvz013

Vesnic-Alujevic, L., Stoermer, E., Rudkin, J.-E., Scapolo, F., & Kimbell, L. (2019). The future of government 2030+. In *Publications Office of the European Union*. https://doi.org/10.2760/145751

Vigoda-Gadot, E. (2002). From responsiveness to collaboration: Governance, citizens, and the next generation of public administration. *Public Administration Review, 62*, 527–540. https://doi.org/10.1111/1540-6210.00235

van der Wal, Z., & van Hout, E. T. J. (2009). Is public value pluralism paramount? The intrinsic multiplicity and hybridity of public values. *International Journal of Public Administration, 32*(3–4), 220–231. https://doi.org/10.1080/01900690902732681

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly, 26*(2), 12.

Weigl, L., Amard, A., Marxen, H., Roth, T., & Zavolokina, L. (2022). User-centricity and public values in E-government: Friend or foe?. In *, 18. 30th European conference on information systems*.

Welby, B. (2019). *The impact of digital government on citizen well-being (32; OECD working papers on public governance)*. https://doi.org/10.1787/24bac82f-en

Wiredu, G. (2012). Information systems innovation in public organisations: An institutional perspective. *Information Technology & People, 25*, 188–206. https://doi.org/10.1108/09593841211232703

Yang, K., & Pandey, S. K. (2011). Further dissecting the black box of citizen participation: When does citizen involvement Lead to good outcomes? *Public Administration Review, 71*(6), 880–892. https://doi.org/10.1111/j.1540-6210.2011.02417.x

Zavolokina, L., Sprenkamp, K., & Schenk, B. (2023). Citizens' expectations about achieving public value and the role of digital technologies: It takes three to tango!. https://hdl.handle.net/10125/102873.

Zucker, L. G. (1977). The role of institutionalization in cultural persistence. *American Sociological Review, 42*(5), 726–743. https://doi.org/10.2307/2094862

Linda Weigl holds a PhD from the Interdisciplinary Center for Security, Reliability and Trust at the University of Luxembourg and is currently a postdoctoral researcher at the Institute for Information Law at the University of Amsterdam. Her research interests lie in digital sovereignty, digital regulation, and trustworthiness in the digital society. Linda focuses on platform regulation and digital trust dynamics of decentralized infrastructures. She further analyzes how technology-centric solutions can be reconciled with democratic criteria and public values.

Tamara Roth is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability, and Trust (University of Luxembourg) and an incoming assistant professor at the Sam M. Walton College of Business (University of Arkansas). Her research focuses on the design and use of IT for social good as well as the role of organizational culture and organizational sensemaking in IT management. Tamara's work spans the individual, organizational, and societal levels. She particularly explores the management and adoption of distributed ledger technologies and the societal implications of digital identities.

Alexandre Amard is a PhD candidate at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT) of the University of Luxembourg. He graduated in International Business Management from Grenoble Graduate Business School and supports public institutions and private operators on their path to digital transformation, with a focus on large-scale systems in the area of digital identity, border management and migration. His research interests lie primarily at the intersection between technology and major societal changes, and in particular with regards to the relationship between citizens, public and private sector.

Liudmila Zavolokina is postdoctoral researcher at the Digital Society Initiative of the University of Zurich (UZH) and an incoming assistant professor at the University of Lausanne. She holds a PhD from the University of Zurich. Her research is design-oriented and focuses on enterprise blockchains, digital trust, and emerging digital technologies—in particular digital platforms and AI—for public value.

Empowering refugees for European bureaucracy: Designing a trustworthy mobile app for document management

Alexandre Amard, Alexandra Hoess, Tamara Roth, Gilbert Fridgen, and Alexander Rieger

Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg
{alexandre.amard, alexandra.hoess, tamara.roth, gilbert.fridgen, alexander.rieger}@uni.lu

Abstract. When arriving in European host countries, refugees need to go through a multitude of administrative processes before they can participate in society. However, these processes are often challenging, as refugees struggle to understand them, lack instructions for managing paperwork, and do not possess the required language skills. Prior research emphasizes the role of information and communication technologies to simplify and enable refugee-friendly administrative processes. However, recent research and existing applications mainly focus on information retrieval and do not offer assistance for understanding official letters, completing administrative forms, and managing corresponding documents. Furthermore, refugees are often reluctant to use existing applications as they do not trust their host country's governments and public authorities. In this research, we aim to address this functional and trust gap. We follow a design science research approach to develop a design for a refugee-centric and trustworthy mobile application that assists refugees along administrative processes. In doing so, we identify three design principles that may guide the development of such applications for refugees.

Keywords: Refugees · Trust · Document Management.

1 Introduction

Global conflicts, human rights violations, and social injustice regularly force enormous numbers of refugees out of their home countries towards Europe [31]. Upon arrival in their European host countries, refugees typically have a hard time participating in and integrating into society [1,2]. Many lack official identity documents, which not only limits their access to public and private services [17], but also requires a series of administrative processes to regain such documents and obtain the right to stay [1]. However, these processes are often hard to complete for refugees due to language barriers, missing instructions, or a lack of understanding of their required contributions [2]. Furthermore, refugees frequently struggle to manage the quantity and diversity of official documents that they receive throughout these processes.

Prior research has emphasized the potential of information and communication technology (ICT) to make such processes more refugee-friendly and lower the barriers to social inclusion [2,17,23]. Research particularly focuses on web and mobile applications that enable refugees to retrieve important information related to administrative processes, healthcare, living, and interaction with the local community in simplified language and with an intuitive design [28,1]. While these applications may be helpful for understanding the structure of administrative processes, they do not currently provide support with document management, ranging from distinguishing and understanding official letters to completing administrative forms and managing corresponding certificates. Consequently, most refugees still depend on the help of refugee assistants to complete administrative processes, which strains refugee assistants and limits agency and perceived self-efficacy of refugees [1]. Research also highlights that refugees often do not trust their host country's public authorities because of negative experiences in their home-, transit- or even host countries [13]. This frequently inhibits the adoption of ICT, as refugees are afraid to use apps provided by public authorities, which might disclose information that had been used for prosecution or suppression in their past [17,27]. As such, trust is a prerequisite to the refugees' adoption of ICT provided by their host countries, and to leveraging the benefits attached to its use.

Adequate ICT solutions for refugees need to consider these concerns in their design. They need to give refugees more agency and control in handling their documents and should foster trust in their host countries' governments [2,8,20]. Acknowledging AbuJarour et al.'s [1] call for further research concerning the design of trustworthy ICT to facilitate administrative processes, this research thus investigates the following research question: *How to design a user-centric and trustworthy mobile application that assists refugees in administrative processes?*

To answer this research question, we follow a Design Science Research (DSR) approach [25] and develop a fit-for-purpose design for a mobile application that assists refugees along administrative processes. In doing so, we build upon work in the area of ICT for refugees as well as institution-based trust. Our design is informed by nine ex-ante interviews with government officials and representatives of public authorities and fourteen ex-post interviews with refugees and refugee assistants, which helped us ensure relevance and rigor. From our final design, we infer three design principles.

2 Background

2.1 The Role of ICT for Refugees

Following their arrival in European host countries, refugees have to complete many administrative processes to obtain a residency permit, access healthcare, or have educational credentials recognized [1]. As an initial step, refugees typically complete an asylum procedure, which entitles them to access such basic services. While refugees are often well-guided throughout the asylum procedure, subsequent processes are challenging [24]. Not least as many administrative processes in European countries are still paper-based [1]. Moreover, they are often complex and may appear arbitrary for those who are not familiar with the system. In particular, refugees often struggle with understanding paperwork, not only because of language barriers but also due to intricate bureaucratic complexities [2,24]. Refugees also often lack information and guidance concerning process steps and those contributions they have to make themselves.

As prior research illustrates, integrating ICT into administrative processes can help refugees navigate integration procedures [1]. Yet, while various applications exist that support refugees in accessing important information and identifying themselves, we could not pinpoint solutions that assist refugees along administrative processes and help them manage official documents. Moreover, we found that many existing applications pay too little attention to accessibility for refugees. This is problematic as refugees may have difficulties using interfaces that do not match their levels of digital literacy or have reading directions that only follow European specifications [28]. Thus, further research is required on refugee-centric design [1].

An approach to such refugee-centric design is the integration of refugee agency [1,2,28]. For instance, mobile apps for refugees can improve accessibility of vital information concerning areas such as healthcare, public administration, education, or every-day live [28]. Moreover, they can digitize administrative forms and lower barriers of understanding for refugees by complementing digital forms with additional instructions. Mobile apps can also support refugees with identification and authentication - an approach currently pursued by the UNHCR [17]. Privacy-preserving applications, so-called digital wallet apps, can even grant independence of public institutions in managing identity-related certificates and documents [5]. These apps promise refugees a high degree of self-efficacy, control, and privacy regarding their identity information [5,26]. Refugee agency and privacy are also important for re-building trust in governments and public authorities as many refugees have made negative experiences with governments that did not uphold either [17,13,6].

2.2 Antecedents of Institution-based Trust

As prior research illustrates, trust and distrust beliefs towards an institution can have a significant impact on the trustee's adoption of digital services and technologies [19]. For our particular research, this effectively means that a successful application for the support of administrative processes and management of official documents has to enhance refugees' institution-based trust and reduce their institution-based distrust.

Trust is commonly associated with "the willingness of a party to be vulnerable to another party's actions based on the expectation that the other party will perform a particular action" [9, p.3]. Most citizens in Europe trust their governments and public authorities to lawfully and reliably deliver public service. However, refugees typically do not have such institution-based trust as they have been prosecuted or suppressed by governments and public authorities in their home countries [9,13].

The formation of such institution-based trust typically depends on three factors: the institution's perceived integrity, the institution's perceived competence for reliable action, and its intention to act in a benevolent manner [20,22]. If a trusting party, such as refugees, believes that an institution will not act with integrity and in a competent and benevolent way, trust will decrease or even be undermined. Such lack of trust may even stimulate the emergence of distrust [20]. Distrust manifests itself when there is a "lack of confidence in the other, a concern that the other may act as to harm one, [. . .] not [caring] about one's welfare [. . .]" [10, p.240]. Like trust, distrust also comprises three dimensions: deceit, incompetence, and malevolence [20,22]. Importantly, a lack of trust does not automatically lead to distrust [22].

3 Research Method

To develop our artifact – a design for a refugee-centric and trustworthy mobile application which we call the "Asylum Wizard" – we adopted a DSR approach [12,25]. In doing so, we followed the proposed DSR process model of Peffers et al. [25]. The process starts with the problem identification. To do so, we conducted nine qualitative and semi-structured ex-ante interviews [29] with government officials and representatives of public authorities that are regularly in touch with refugees. With these interviewees, we discussed problems that refugees typically encounter while dealing with administrative processes. We identified a lack of refugee agency in managing their official documents and completing administrative processes as an important problem. We also established the existence of weak trust or even distrust beliefs in governments and public authorities. Thus, this research intends to develop a refugee-centric design that enhances agency and mediates trust concerns by supporting refugees in effectively managing their official documents.

Subsequent to our problem description, we structured and condensed our insights into *design requirements* – generic requirements that any artifact aiming to solve the underlying problem class should meet – for an application that could assist refugees [7,21,30]. In addition to the interviews, which ensure the practical relevance of our research, we consulted prior literature on the role of ICT for refugees and institution-based trust and distrust. This warrants the rigor, validity, and effectiveness of our research [34,35].

Based on the design requirements, we developed and iteratively refined our DSR artifact. We first translated the identified requirements into design features which represent the technical specifications and components of our solution [7,21]. Thereafter, we instantiated the design features into a paper-based prototype of our "Asylum Wizard", to help demonstrate our design.

For the demonstration, we presented the paper-based prototype to refugees and refugee assistants and discussed with them the *design features* of our solution. These interviews also served as a basis for the evaluation of our design [32]. Overall, we conducted 14 ex-post interviews with three refugees and eleven refugee assistants – who support refugees along administrative processes on a regular basis – to gain feedback from an end-user perspective. In particular, we discussed the design features and the Asylum Wizard's usability and trust-enhancing qualities, as well as potentials for improvement. After each interview, we evaluated the feedback and adapted our design features and paper-based prototype, if necessary. The interviews enabled us to abstract our design into *design principles* that provide explanations for how our design features address the identified design requirements and provide a solution to our underlying problem class [7]. More specifically, the design principles offer generalizeable guidelines on how to design applications that assist refugees along administrative processes and generic capabilities that may technically support trust [3,11,21].

4 Design and Development

4.1 Design Requirements

Our ex-ante interviews as well as the literature on the role of ICT for refugees and institution-based trust and distrust provided us with overall six design requirements for our Asylum Wizard. More specifically, they highlighted the potential for increased refugee agency through the use of ICT [18,23]. Most refugees are currently relying on information provided by government officials or refugee assistants without the ability to "fully participate [. . .] and control their own destinies" [2, p.406]. This does not only create exclusion from the society of their host countries but also takes a mental toll on refugees who find it "difficult to accept help – from a cultural perspective – as they do not want to appear weak" (Gov 7). Thus, granting refugees *control of documents and information flows* (DR 1) is a cornerstone of a refugee-centric ICT design that helps prevent the development of distrust beliefs towards host governments and supporting organizations [6]. An *increased availability of relevant documents for refugees* (DR 2) helps them navigate unfamiliar government procedures and information environments [6,15]. To date, refugees often do not know "what they have to fill in, why they have to fill it in, and where to put the filled in document" (Gov 1). *Indications of completeness of documents* (DR 3) and an *overview of documents and information flows* (DR 4) may enable refugees to better understand these requirements, the current state of their respective procedure, and for which documents their identity-related information is needed. *Understanding the required documents and processes* (DR 5) also helps refugees to be "much more accepting of administrative processes – regardless of how positive or negative the outcome" (Gov 5). Thus, knowledge and understanding can ensure refugees' trust in the integrity of government agencies and supporting organizations. An *increased efficiency of data exchange for refugees* (DR 6) may also improve the interaction with and perceived competence of government officials and representatives of public institutions, and thus the trust they place in them. Indeed, should documents be lost or incomplete, refugees may more easily find the "receipt that shows [that] documents have been complete upon submission" (Gov 5).

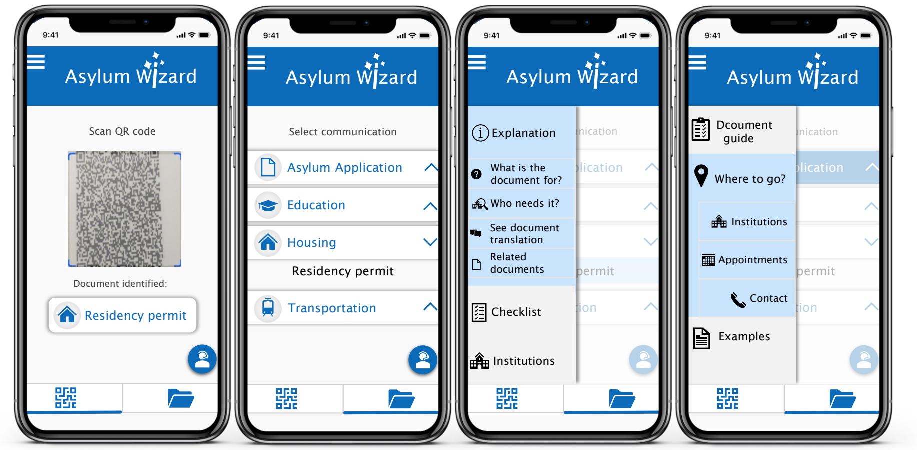


Fig. 1. Design of the Asylum Wizard.

4.2 Design Features and Instantiation

Guided by our design requirements, we developed design features that were directly relevant for the design of our refugee-centric and trustworthy mobile application [21]. Overall, we identified eleven design features, which either directly concerned document management or increased agency as well as inclusive or culture-specific adaptations of our Asylum Wizard. As a first step towards more knowledge about governmental procedures in their host country, *explanations of unknown procedures* (DF 1) is an important design feature. That is, information in official documents, which is often hidden behind formal bureaucratic language to conform with formal requirements of government documents [4], is didactically reduced to the essential points. To access this information, official documents can be enhanced with QR-codes. Refugees can scan a QR-code provided on a paper-based document with their Asylum Wizard that *automatically allocates* (DF 2) a digital version of the document into *pre-structured document folders* (DF 3) within the asylum application (Figure 1). These folders concern key areas in the refugees' journey through the adminsitrative processes of their host country, for instance housing, transportation, or the asylum procedure [1,28]. Since refugees "[often] have no idea of folder structures" (RA 5), the pre-structured folders also help refugees to organise their physical documents in folders. In case of successful submission or presentation, another QR-code provided on the receipt issued by responsible government agencies can mark the respective digital document as completed by changing its color to green. This constitutes the *integration of a checklist* (DF 4) to help refugees assess their progress in a procedure and understand the relevant details. Such checklists could also provide information on the due date of document submissions and the intended recipient of a document.

While this design may already allow for more agency, refugee applications also need to *consider different levels of literacy* (DF 5), i.e., not all refugees can read and write [15,26]. To limit discrimination, refugees can choose between written language and sign language combined with audios as basic settings. In both cases, availability of the refugees' native languages is important. This not only includes translations of all information but also *culturally appropriate presentation of information* (DF 6) – such as where information is being provided – to make the user journey more intuitive. Likewise, automation and a simple interface enable the *consideration of different levels of digital literacy* (DF 7). Many refugees are not familiar with using digital devices [15,33], which is why we decided for an inclusive design.

Inclusive design also extends to the consideration of the refugees' fears and concerns. More specifically, many refugees fear that the use of apps, such as the Asylum Wizard, would allow for tracking of personal information [6]. To address those fears, features of secure digital wallet apps and decentralized digital identities can be included. Comparable to a physical wallet, secure digital wallets can guarantee the *privacy of documents* (DF 8) thanks to methods such as encryption and access management, which provides refugees with more control and may reduce the perceived malevolence of governments [5,6]. Due to the intuitive and clear folder structure, refugees could also better *control document sharing and disclosure* (DF 9), while the use of QR-codes on documents could include features for *verifying the integrity of documents* (DF 10). Finally, providing an overview of the documents they need and what they are required for, as well as when they have submitted their documents to the competent person or authority, enables additional *transparency over processing of disclosed documents* (DF 11). Thus, at all points in time, refugees are aware of what happens with their documents and how many documents they still need to complete.

5 Evaluation

In the evaluation interviews, we asked refugee assistants (RA) and refugees (R) in how far they deem the presented Asylum Wizard as trust-enhancing and what other functions they believed would further increase the perceived trustworthiness of our application. Both groups highlighted the intuitive organization of the pre-structured document folders (DF 3). They again emphasized that refugees have difficulties identifying relevant documents – some would appear with the entire contents of their mailbox including newsletters and adverts – and are unable to put these documents into a coherent order (RA 4, 10/11). They particularly appreciated the possibility to automatically allocate documents to pre-structured folders (DF 2) with the help of a QR-code (DF 10). Such an allocation would prevent them from saving irrelevant documents or discarding relevant ones (R 1 - 3; RA 1, 2, 4 - 6, 8, 10/11), making them feel less vulnerable and more confident in their interaction with public authorities.

Refugee assistants also emphasized that being able to check the completeness of application documents and keep track of submission deadlines (RA 4, 5) during the asylum application were indeed valuable features. With incoming documents often referring to more or less the same procedure, refugees felt that a transparent overview would increase their understanding and agency. In addition to more integration-related sub-folders, we therefore also included the checklist function for asylum application documents (DF 4). Moreover, both refugees and refugee assistants suggested the addition of a status-tracing function in the Asylum Wizard (RA 4 - 6, 10/11). This would increase transparency for refugees throughout the asylum procedure (DF 11), making it more understandable where they are in the procedure and when they could expect a decision (DF 1) (R 2 - 3). Such transparency would greatly add to clarity and positive beliefs. At the same time, refugees voiced concern that using an app with a status-tracing function would reveal information about them that they do not wish to share, and thus appreciated the inclusion of privacy and control features (DF 8, DF 9). Since many refugees are not aware of their host countries' privacy and data protection regulations or the legal obligations of those countries' governments, privacy assurance would either require extensive explaining or a technology-mediated guarantee (RA 2, 4, 6, 7, 10/11). Overall, many refugee assistants and most refugees would prefer technology-mediated guarantees, in which refugees may trust more than in governments. For explanations of documents and procedures, interviewees collectively appreciated the simplification of content as an addition to official documents (DF 1) as well as the consideration of different levels of (digital) literacy (DF 5, DF 7) to increase understanding and the availability of information. As documents must still be filled in manually, refugees suggested reference examples as part of the explanation for each document in their target languages to make it easier for them to fill in the forms (DF 1, DF 6) (R 1 - 3).

6 Discussion

We consolidated the iterations and evaluations of our design with refugee assistants and refugees in a nascent design theory, i.e. in generalizable design principles [3,11]. We have identified three design principles that provide knowledge on how to design technical applications that help restore institution-based trust [20,22] and mediate institution-based distrust [14,19] of refugees (Figure 2 & 3). We add to theory by proposing that aside from inclusive or culture-sensitive design, document management and increased agency may be trust-enhancing factors. Furthermore, our design principles may provide potential solutions for practitioners who wish to develop applications for refugees that build on the same underlying class of problems.

DP1 – Guided document management: When evaluating the refugee assistants' and refugees' feedback, we found that distrust beliefs in governmental agencies [6] based on incomplete documents or repetitive requests can be mediated by having a mobile document management application. This would not only support refugees in allocating official documents to dedicated folders but would also help them understand the purpose and content of such documents, potentially breaking the cycle of distrust. Imparting knowledge of the procedures and requirements in an accessible manner would put refugees in a position of control. With increased control, refugees may not only reduce their distrust beliefs

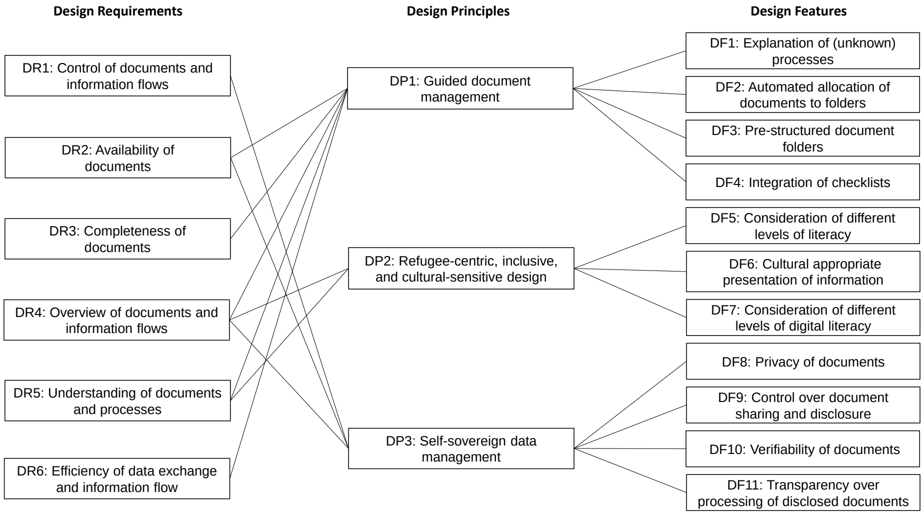

Design Requirements
Design Principles
Design Features
DR1: Control of documents and information flows
DR2: Availability of documents
DR3: Completeness of documents
DR4: Overview of documents and information flows
DR5: Understanding of documents and processes
DR6: Efficiency of data exchange and information flow
DP1: Guided document management
DP2: Refugee-centric, inclusive, and cultural-sensitive design
DP3: Self-sovereign data management
DF1: Explanation of (unknown) processes
DF2: Automated allocation of documents to folders
DF3: Pre-structured document folders
DF4: Integration of checklists
DF5: Consideration of different levels of literacy
DF6: Cultural appropriate presentation of information
DF7: Consideration of different levels of digital literacy
DF8: Privacy of documents
DF9: Control over document sharing and disclosure
DF10: Verifiability of documents
DF11: Transparency over processing of disclosed documents

Fig. 2. Overview of design requirements, principles, and features.

but may be able to better assess bureaucratic requirements and the integrity and competence of governmental procedures, and thereby also build institution-based trust [19,20,22]. The additional checklist function of our Asylum Wizard further emphasizes the refugees' position of control. Having something that would not only indicate the completeness of a document but also due dates and receiving parties, creates a feeling of safety, which in turn also increases the institutions' perceived benevolence and competence. This, in turn, positively affect the formation of institution-based trust [20,22].

DP2 – Refugee-centric, inclusive & cultural-sensitive design: Although a more general prerequisite of all applications – physical or digital – refugee-centric design is pivotal in building trust-relations. Newly arriving refugees lack a sense of belonging and agency [16]. In many cases, this sense of alienation and dependency is further emphasized by language barriers. To counteract this trend and bridge the comprehension gap despite the lack of language competencies of many refugees, the Asylum Wizard offers a didactically reduced and culturally appropriate design of information presentation [16]. This way, refugees may feel less alienated and more capable to act as they find their needs represented regardless of literacy levels. The same also applies to digital literacy, where automation of key processes, and easy and intuitive icons should prevent less digitally literate refugees from feeling overwhelmed [26]. Overall, positive experiences with the Asylum Wizard and a sense of belonging through culturally appropriate design and representation may foster the belief of benevolence and reduce distrust and fears of malevolence [19,22].

DP3 – Self-sovereign data management: Gaining more control through understanding and being able to handle one's own data is also closely connected to self-sovereignty and empowerment principles [8]. By building on best practices

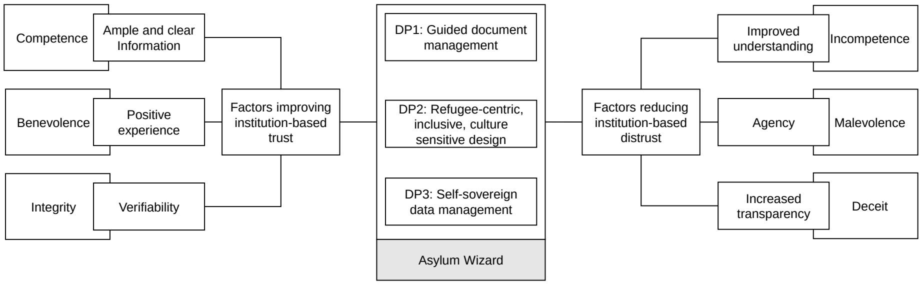

Competence
Ample and clear Information
Benevolence
Positive experience
Integrity
Verifiability
Factors improving institution-based trust
DP1: Guided document management
DP2: Refugee-centric, inclusive, culture sensitive design
DP3: Self-sovereign data management
Asylum Wizard
Factors reducing institution-based distrust
Improved understanding
Incompetence
Agency
Malevolence
Increased transparency
Deceit

Fig. 3. Design principles for a trust-enhancing design.

from digital wallet apps, the Asylum Wizard could ensure that data stored in the app remains private and in the hands of the refugees [8,26]. Yet, it would also make it possible to share this data with other refugees or trusted refugee assistants in a self-controlled manner to, for instance, provide them with additional samples for filling in documents. Moreover, refugees may share their filled in documents with competent government officials before submission to make sure that the documents are complete. This again may improve the refugees' relative power position and could make them feel more self-sufficient. At the same time, their increased sovereignty may positively reflect on heightened competence beliefs regarding their host country's government and may thus foster institution-based trust [20,22]. Increased transparency through knowledge about processes and having all relevant information available and verified in their app further improves such trust through positive perceptions of the government's integrity and benevolence [19,22].

7 Conclusion

In this study, we discuss how a mobile application that assists refugees in administrative processes can be built in a refugee-centric and trustworthy manner. In a DSR approach based on literature about ICT for refugees and institution-based trust and distrust as well as stakeholder interviews, we infer three design principles from our Asylum Wizard. We find that guided document management and refugee-centric, inclusive, and cultural-sensitive design may help reduce institution-based distrust; it may even increase institution-based trust when combined with self-sovereign data management. Yet, this effect may depend on the refugees' understanding of the underlying technology to appreciate that (1) governments intend to improve the trust relationship by (2) providing the app. Overall, our DSR-based design principles and design features to a refugee-centric Asylum Wizard may help researchers and practitioners alike to understand the complex interplay of trust and distrust factors in designing trustworthy and user-centric applications for refugees.

Acknowledgments: This research is supported by PayPal and the Luxembourg National Research Fund FNR, Luxembourg (P17/IS/13342933/PayPal-FNR/Chair in DFS/ Gilbert Fridgen) as well as by the Luxembourg National Research Fund (FNR) – FiReSpARX Project, ref. 14783405

References

1. AbuJarour, S., Wiesche, M., Andrade, A.D., Fedorowicz, J., Krasnova, H., Olbrich, S., Tan, C.W., Urquhart, C., Venkatesh, V.: Ict-enabled refugee integration: A research agenda. Communications of the AIS **44**(1), 874–891 (2019)
2. Andrade, A.D., Doolin, B.: Information and communication technology and the social inclusion of refugees. Mis Quarterly **40**(2), 405–416 (2016)
3. Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., Rossi, M.: Design science research contributions: Finding a balance between artifact and theory. Journal of the Association for Information Systems **19**(5), 3 (2018)
4. Bundesamt für Migration und Flüchtlinge: DA-Asyl (2019), `https://www.proasyl.de/wp-content/uploads/DA-Asyl_21_02_2019.pdf`
5. Bundesamt für Migration und Flüchtlinge: Digitalisierung der Bescheinigungsprozesse im Asylverfahren mittels digitaler Identitäten (2021), `https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper-2021.pdf?__blob=publicationFile&v=3`
6. Carlson, M., Jakli, L., Linos, K.: Rumors and refugees: how government-created information vacuums undermine effective crisis management. International Studies Quarterly **62**(3), 671–685 (2018)
7. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., Wortmann, F.: Blockchain for the iot: privacy-preserving protection of sensor data. Journal of the Association for Information Systems **20**(9), 1274–1309 (2019)
8. Cheesman, M.: Self-sovereignty for refugees? the contested horizons of digital identity. Geopolitics **27**(1), 134–159 (2022)
9. Cheng, X., Fu, S., de Vreede, G.J.: Determinants of trust in computer-mediated offshore software-outsourcing collaboration. International Journal of Information Management **57**, 102301 (2021)
10. Govier, T.: Is it a jungle out there? trust, distrust and the construction of social reality. Dialogue: Canadian Philosophical Review/Revue canadienne de philosophie **33**(2), 237–252 (1994)
11. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS quarterly pp. 337–355 (2013)
12. Hevner, A., March, S.T., Park, J., Ram, S., et al.: Design science research in information systems. MIS Quarterly **28**(1), 75–105 (2004)
13. Hynes, T.: The issue of 'trust' or 'mistrust' in research with refugees: choices, caveats and considerations for researchers (2003), `https://www.unhcr.org/research/RESEARCH/3fcb5cee1.pdf`
14. Kramer, R.M.: Trust and distrust in organizations: Emerging perspectives, enduring questions. Annual review of psychology **50**(1), 569–598 (1999)
15. Lloyd, A., Kennan, M.A., Thompson, K.M., Qayyum, A.: Connecting with new information landscapes: information literacy practices of refugees. Journal of Documentation (2013)
16. Lyytinen, E.: Refugees''journeys of trust': Creating an analytical framework to examine refugees' exilic journeys with a focus on trust. Journal of Refugee Studies **30**(4), 489–510 (2017)

17. Madon, S., Schoemaker, E.: Digital identity as a platform for improving refugee management. Information Systems Journal (2021)
18. Majchrzak, A., Markus, M.L., Wareham, J.: Designing for digital transformation: Lessons for information systems research from the study of ict and societal challenges. MIS quarterly **40**(2), 267–277 (2016)
19. McKnight, D.H., Choudhury, V.: Distrust and trust in b2c e-commerce: do they differ? In: Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet. pp. 482–491 (2006)
20. McKnight, D.H., Lankton, N.K., Nicolaou, A., Price, J.: Distinguishing the effects of b2b information quality, system quality, and service outcome quality on trust and distrust. The Journal of Strategic Information Systems **26**(2), 118–141 (2017)
21. Meth, H., Mueller, B., Maedche, A.: Designing a requirement mining system. Journal of the Association for Information Systems **16**(9), 2 (2015)
22. Moody, G.D., Lowry, P.B., Galletta, D.F.: It's complicated: explaining the relationship between trust, distrust, and ambivalence in online transaction relationships using polynomial regression analysis and response surface analysis. European Journal of Information Systems **26**(4), 379–413 (2017)
23. Nedelcu, M., Soysüren, I.: Precarious migrants, migration regimes and digital technologies: The empowerment-control nexus. Journal of Ethnic and Migration Studies pp. 1–17 (2020)
24. Pearlman, W.: Culture or bureaucracy? challenges in syrian refugees' initial settlement in germany. Middle East Law and Governance **9**(3), 313–327 (2017)
25. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. Journal of Management Information Systems **24**(3), 45–77 (2007)
26. Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., Fridgen, G.: Not yet another digital identity. Nature human behaviour pp. 1–1 (2021)
27. Schoemaker, E., Baslan, D., Pon, B., Dell, N.: Identity at the margins: data justice and refugee experiences with digital identity systems in lebanon, jordan, and uganda. Information Technology for Development **27**(1), 13–36 (2021)
28. Schreieck, M., Zitzelsberger, J., Siepe, S., Wiesche, M., Krcmar, H.: Supporting refugees in everyday life-intercultural design evaluation of an application for local information. PACIS 2017 Proceedings (2017)
29. Schultze, U., Avital, M.: Designing interviews to generate rich data for information systems research. Information and organization **21**(1), 1–16 (2011)
30. Siering, M., Muntermann, J., Grčar, M.: Design principles for robust fraud detection: The case of stock market manipulations. Journal of the Association for Information Systems **22**(1), 4 (2021)
31. UNHCR: UNHCR 2020 Global Report (2021), `https://reporting.unhcr.org/download?origin=gtgrpage&file=gr2020/pdf/GR2020_English_Full_lowres.pdf`
32. Venable, J., Pries-Heje, J., Baskerville, R.: FEDS: A framework for evaluation in design science research. European Journal of Information Systems **25**(1) (2016)
33. Vollmer, S.: Syrian newcomers and their digital literacy practices. Language Issues: The ESOL Journal **28**(2), 66–72 (2017)
34. Vom Brocke, J., Winter, R., Hevner, A., Maedche, A.: Special Issue Editorial – Accumulation and evolution of design knowledge in design science research: A journey through time and space. Journal of the Association for Information Systems **21**(3), 9 (2020)
35. Winter, R.: Design science research in europe. European Journal of Information Systems **17**(5), 470–475 (2008)

Chapter 4
Decentralized Digital Identities

Alexandre Amard, Pol Hölzmer, Alexandra Hoess

Abstract In the financial sector, regulatory requirements impose stringent rules related to the identification of customers and the management of their identity data. Financial institutions not only need to comply with strict requirements with regard to know-your-customer (KYC) processes and customer authentication but also with legislation pertaining to the management of personal data, e.g., related to data protection and minimization. Decentralized digital identities in the form of digital identity wallets represent an alternative to the traditional identity management model, in which organizations often collect more data than necessary for the provisioning of services and struggle to verify it efficiently and effectively. Digital identity wallets enable systemic trust and give control of identity data back to the data subject. In this chapter, we outline the technical means through which such decentralized digital identities can enable high degrees of user control, identity assurance, and privacy. We cover the governance and technical aspects of digital wallet-based decentralized digital identity management and outline the challenges ahead to realize their full potential.

Alexandre Amard
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg
29 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
e-mail: `alexandre.amard@uni.lu`

Pol Hölzmer
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg
29 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
e-mail: `pol.hoelzmer@uni.lu`

Alexandra Hoess
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg
29 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
e-mail: `alexandra.hoess@uni.lu`

4.1 Introduction

With the increasing digitalization of our societies and economies, digital identity has become one of the main foci to translate trusted identity management (IdM) from the physical world to the digital world. In fact, "the Internet was built without a way to know who and what [people] are connecting to" (Cameron, 2005). Although organizations and hardware have had innate ways to identify themselves since the early days of the Internet (by different means such as the *address resolution protocol (ARP)*, *medium access control (MAC) addresses*, *domain name services (DNS)*, or *cryptographic certificates*), end users mainly relied on ad hoc identity management (Gaedke et al., 2005).

The relevance of digital identity management is particularly exemplified in the financial sector, where regulations impose stringent requirements for customer identification (Schlatt et al., 2022). To open a bank account, KYC processes that involve the collection of identity data, are considered fundamental to market integrity concerning anti-money laundering (AML) and countering the financing of terrorism objectives (Arner et al., 2019). Also, specific levels of authentication strengths are often legally required to digitally access a bank account and validate payment orders to protect customers and reduce fraud (e.g., the Revised Payment Services Directive (PSD2)) (Fabcic, 2021). On top of these requirements, financial service providers need to comply with legislation on managing and protecting personal data. These requirements are increasingly being enforced in various regions of the world (e.g., the General Data Protection Regulation (GDPR) in the European Union (EU)) (De Hert et al., 2018), imposing additional safeguards on the management of identity data.

Historically, digital identity management systems have relied on users to provide different sets of personal data to each online service they joined, and these services would store and manage this information (Sedlmeir et al., 2022a). Although functional, this approach has significant drawbacks. It relies either on non-verified attributes or on certified attributes originating from physical identity documents. Transmitting these certified attributes often requires users to make copies of their identity documents and send them to the service provider. This is problematic for several reasons. First, service providers do not have a convenient way to verify that this shared information can be trusted (Lacity et al., 2023). When they do check, this verification entails a query to the identity document issuer, which leaves a trace in the trust infrastructure that can be used to track a user's interaction with a service. Furthermore, most identity documents do not allow for selective disclosure of attributes, thus leaking more data than required. Finally, identity documents are often shared via insecure communication channels, such as unencrypted email.

More recently, the federated identity management paradigm became dominant, where an identity provider collects and stores identity data and acts as an intermediary between the user and service providers (Maler and Reed, 2008; Sedlmeir et al., 2021). This approach improves convenience for users, who only need to do it once for all the federated services instead of providing their identity data for each service provider. However, this paradigm does not alleviate privacy concerns. On the contrary, it increases the amount of identity data the user shares for accessing the service, remarkably increasing the potential for aggregation of this information by identity providers. This, in turn, enables them to personal data for additional purposes such as marketing, profiling, or even surveillance purposes (Preukschat and Reed, 2021).

Decentralized digital identities were designed as a response to these shortcomings. They allow users to store their own certified identity attributes, share them through secure communication channels, and prove their integrity and authenticity without the certification authority knowing about it. Often also coined self-sovereign identity (SSI) (Allen, 2016), this concept embodies the principle that individuals should have control of the disclosure of their identity attributes without relying on any centralized authority. Instead, this user-centric model (Weigl et al., 2022) uses machine-verifiable attestations stored in users' digital identity wallets and is supplemented by a trust infrastructure. Importantly, with the incorporation of data minimization techniques such as zero-knowledge proofs (ZKPs), users can specify which information to disclose without hampering verifiability (Babel and Sedlmeir, 2023). In essence, they significantly improve on the previous paradigms from a security and data protection standpoint while granting more control to the user.

Recognizing the benefits of a more user-centric identity management system based on a privacy-respecting paradigm, in June 2021, the EU started its revision of its electronic Identification, Authentication and Trust Services (eIDAS) regulation which harmonized national electronic identity (eID) frameworks across member states in 2014. Its purpose is to massively extend the use of electronic identification from public to private services by introducing a nationally endorsed and interoperable European digital identity wallet (EUDIW) for the 450 million EU citizens, based on the paradigm of decentralized digital identities (Weigl et al., 2023).

In line with these premises, this chapter outlines the technical means through which decentralized digital identities can support user control and data minimization, marking a shift towards more user-centricity, helping to prevent tracking and identity theft while still providing high levels of assurance for identity verification (Sedlmeir et al., 2021). It also elaborates on the possibility of decoupling the relationship between attestation issuers (e.g., governmental entities) and verifiers (e.g., financial service providers), thus limiting the risk of collusion and surveillance while guaranteeing the same level of identity assurance. Finally, it outlines the key building blocks required for decentralized digital identity management and presents the challenges ahead on the way to fully transitioning to a decentralized digital identity management paradigm.

4.2 Decentralized Digital Identity Ecosystems

Decentralized digital identities represent a noteworthy advancement for digital identity management, as they grant equivalent assurance to today's physical identity management while providing data subjects with high degrees of control and privacy of their identity data. This novel identity management paradigm relies on digital attestations, which are the digital equivalent of traditional plastic cards and paper-based certificates. It combines technology with convenience (Richter et al., 2023). Decentralized digital identity ecosystems involve a set of processes and components, as well as actors. The exchange of digital attestations between issuers, holders, and verifiers happens through secure bilateral (peer-to-peer (P2P)) communication channels that rely on modern cryptography (Mühle et al., 2018). Issuers certify specific attributes and issue a digital attestation about a subject to a holder. Holders store and manage these digital attestations through a so-called digital identity wallet (Sartor et al., 2022; Guggenberger et al., 2023). Upon request by a verifier, they can present their digital attestation or prove specific identity attributes through a machine-verifiable presentation. To validate such a presentation, verifiers commonly check the attestation's signature, expiration date, and state of revocation (Schlatt et al., 2022; Lacity et al., 2023). In doing so, verifiers typically rely on public registries that are embedded in larger "trust infrastructures", which provide additional information that allows for verifying a digital attestation's issuer and state of revocation (Davie et al., 2019). Figure 4.1 illustrates the processes, components, and actors involved in a decentralized digital identity management system. This chapter continues by elaborating on the details of the core technical building blocks underlying such a system, namely public key cryptography, digital attestations, digital identity wallets, and trust infrastructures.

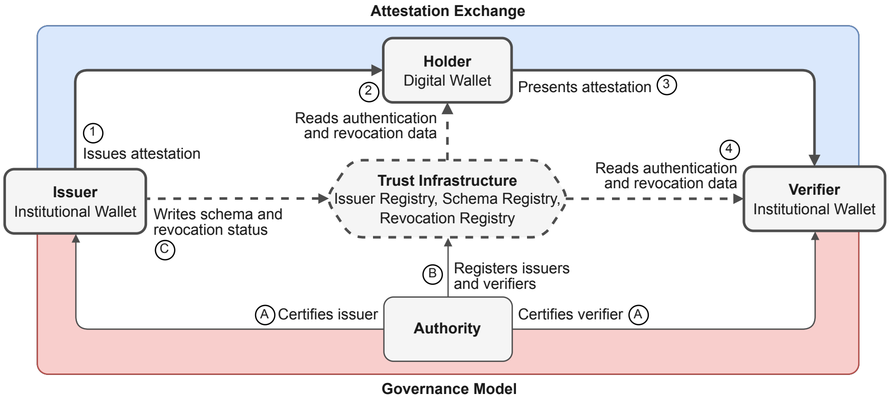


Fig. 4.1 Stakeholder roles and interactions in decentralized digital identity systems.

4.3 Cryptographic Foundations

In the digital age, the trustworthiness of digital identities depends on the strength of their security mechanisms. At the heart of these trust assurances are cryptographic primitives, ranging from encryption to digital signatures. The use of cryptography has profound implications in the domain of decentralized digital identities for proving ownership and correctness of attestations using digital signatures. As we move through the rest of this chapter, understanding how these cryptographic foundations build and maintain trust in digital identities is essential.

Historically, symmetric key cryptography (SKC) has been used for centuries (Luciano and Prichett, 1987). Notably, Julius Caesar already utilized a simple shift cipher to secure his messages during wartime. In general, SKC employs simple permutation (reordering bits) and substitution (replacing bits) operations in combination with a single shared secret key (*k*) for both encryption and decryption. Known for its efficiency, symmetric encryption is often the choice for bulk data protection at rest or in transit. However, key establishment and management present considerable challenges, especially when building trust relations with unknown entities, as identity cannot be verified, actions can be repudiated, and forward secrecy is not guaranteed.

In the realm of cryptography, one of the groundbreaking advancements that emerged in the 1970s is public key cryptography (PKC), also known as asymmetric key cryptography (Diffie and Hellman, 1976). Unlike traditional SKC, PKC employs a pair of distinct keys: a secret key (*sk* – also called a private key) and a corresponding public key (*pk*), hence the term "asymmetric". The secret key is kept securely by the individual or entity, while the public key can be openly shared with others and can function as a public identifier.

PKC has several unique applications due to its asymmetric properties rooted in discrete mathematics. The most important property is that encrypted data using a *pk* can only be decrypted using the corresponding *sk*. Thus, anybody can initiate a secure channel with the owner of the *pk*, who is the only entity able to read the corresponding messages. In doing so, the confidentiality of information can be ensured. In turn, digital signatures are created with a *sk* and can only be verified using the *pk*. In other terms, signatures can only be created by the holder of the *sk* but verified by anyone with the *pk*. That way, the integrity and authenticity of information can be ensured. Those two rather simple concepts provide the baseline security principles described by the "CIA triad" representing confidentiality, integrity, and authenticity.

Despite covering theoretical security principles, PKC lags behind in applied cryptography (BSI, 2023). Here, its limitations become evident: slow operations, suitability for small amounts of data, and the necessity for a dedicated trust infrastructure to distribute public keys. Therefore, PKC is almost explicitly limited to symmetric key establishment and digital signatures. The RSA (Rivest-Shamir-Adleman) cryptosystem (Rivest et al., 1978) is a well-established representative whose security is based on the difficulty of the integer factorization problem (IFS). Today, RSA is mostly superseded by the more efficient elliptic curve cryptography (ECC), whose security relies on the elliptic curve discrete logarithm problem (ECDLP). Noteworthy related algorithms include (EC)DH (Diffie-Hellman) derivates for the symmetric key establishment and (EC)DSA (Digital Signature Algorithm) for digital signatures (BSI, 2023).

In modern systems, SKC and PKC go hand-in-hand to leverage each other's strengths and compensate for weaknesses. It is worth noticing that "security by obscurity" is not a robust or sustainable security strategy and that Kerckhoff's principles (Kerckhoffs, 1883) should always be applied. The core principle states that the security of a cryptographic system should not rely on the secrecy of the algorithm; instead, it must solely depend on the strength of the employed key.

Unfortunately, the IFS and discrete logarithm problem (DLP), which define the strength of many modern asymmetric keys, can be broken quickly using quantum computers, urging the transition to post-quantum cryptography (PQC) even though this vulnerability cannot be exploited yet because current quantum computers still lack the required amount of quantum bits to leverage related attacks. This threat will nevertheless become a reality for PKC in the following years. SKC, in turn, can easily counterweight this threat by increasing the key size by a reasonable amount. In most scenarios, the impact is low, even without countermeasures. To explore similar future-proof solutions for PKC, the National Institute of Standards and Technology (NIST) launched the PQC Standardization program in 2017 (NIST, 2017), which is now in the final round. Current promising candidates for post-quantum secure algorithms include Kyber for symmetric key establishment and Dilithium for digital signatures.

4.4 Digital Attestations

Whereas PKC serves as the technical basis for encryption and digital signatures, digital attestations represent the central building block in which identity information is packaged and exchanged between entities (Lacity et al., 2023). In essence, digital attestations function as the digital analogs of conventional physical identity documents and paper-based certificates, representing a convergence of traditional authentication mechanisms with contemporary cryptographic technologies (Preukschat and Reed, 2021).

Technically, these attestations are digitally signed sets of information that certify one or more identity attributes about a subject (Sedlmeir et al., 2021). Digital attestations typically consist of three main elements: metadata, a set of attributes, and cryptographic proof (W3C, 2023). The *metadata* contains a set of information that specifies when and by whom an attestation has been attested. Digital attestations can be either self-issued, which means the subject creates and signs a digital attestation about oneself, or attested and signed by a third party. The verifier has to decide if self-issued attestations are accepted. Furthermore, the metadata provides information on how an attestation can be verified, i.e., by referencing the trust infrastructure that holds information on how to interpret the information stored in an attestation or whether an attestation has been revoked or not (Glöckler et al., 2023).

Identity attributes form the core of any digital attestation. This is the part that defines the actual identity. It certifies specific characteristics about the identity subject's identity, such as the last name or date of birth. In most cases, the subject of these attributes will also act as a holder who controls the digital attestation. However, in some cases, the subject and the holder may differ. For instance, for a minor's digital ID card, a parent (holder) could act as a guardian and manage a digital attestation on behalf of their child (subject). In any case, holders store and control the digital attestations and present them to a verifier (Weigl et al., 2022). To ensure the integrity of the presented information, digital attestations contain a *cryptographic proof* in the form of a digital signature or an electronic seal. Digital signatures and electronic seals thereby serve two key features: they make digital attestations tamper-evident and allow verifiers to authenticate the attestation issuer cryptographically.

Digital attestations can be presented online and offline by a subject to a verifier (Schlatt et al., 2022). Doing so, a machine-verifiable presentation of an attestation can be created in three different ways: 1) by presenting the whole set of attributes contained within an attestation; 2) by selectively disclosing one or a subset of attributes attested in an attestation, while often still exposing more information than requested by the verifier; or 3) by applying cryptographic ZKPs that allow one to prove an identity attribute to another entity without disclosing any more information than required (Babel and Sedlmeir, 2023; Goldreich and Oren, 1994). For instance, one could prove to meet a certain legal age requirement without providing any further information about one's current age or date of birth. The use of ZKPs is particularly advisable to minimize or avoid the disclosure of sensitive and correlatable data, such as unique cryptographic identifiers. Note that a holder's public keys, as well as an attestation's digital signature, are considered to be a (unique) identifier due to their characteristics and collision resistance. While creating a machine-verifiable presentation, data subjects are not limited in their information disclosure to attributes and information stored within a single digital attestation. Instead, a presentation may also combine information from multiple attestations (Preukschat and Reed, 2021). Yet, as of now, a prerequisite is that these attestations rely on the same technical standard.

Current prominent technical standards for digital attestations include the World Wide Web Consortium's (W3C) Verifiable Credentials (W3C, 2023) and the ISO/IEC 18013 (mdoc) standard for electronic attestations (ISO/IEC, 2021). Although the latter has been particularly developed for the use case of a mobile driver's license, both standards can be widely applied in different domains and use cases. Both standards will also form the technical basis for digital attestations in the EUDIW that the EU is currently developing (European Commission, 2023).

4.5 Digital Identity Wallets

Decentralized digital identity implementations emerged to empower data subjects to regain control of their digital identities (Allen, 2016; Weigl et al., 2022). Consequently, the pivotal elements of any decentralized digital identity implementation are the technologies that allow holders to store and manage digital attestations by themselves. Digital identity wallets play a central role in managing digital identities, as they integrate these technologies and make them accessible to end users (Rieger et al., 2022).

Digital identity wallets are mobile or web-based software applications that act as secure storage for that holder's digital attestations and cryptographic keys (Sartor et al., 2022). They provide features for secure communication and managing digital attestations, such as authenticating other entities based on their public keys, establishing secure connections through PKC, creating digital signatures, receiving digital attestations, and, not least, generating presentations thereof that can be shared and verified in online and offline interactions (Lacity et al., 2023). To ensure privacy-preserving digital identity management, digital identity wallets can be equipped with advanced cryptographic features that, for instance, allow users to generate a new pseudonymous cryptographic keypair for interaction with each new counter-party or to create presentations using ZKPs (Sedlmeir et al., 2022a). Furthermore, digital identity wallets connect to trust infrastructures that provide relevant data for issuer and verifier authentication as well as generating proofs of attestation non-revocation (Feulner et al., 2022; Preukschat and Reed, 2021).

On par with holders' digital identity wallets, institutional wallets provide organizations with technical capabilities for decentralized digital identity management (Schlatt et al., 2022). Institutional wallets (often also referred to as enterprise wallets or agents) are software applications that can be integrated into an organization's IT infrastructure (Lacity et al., 2023; Preukschat and Reed, 2021). They allow organizations to manage their cryptographic keys and establish secure connections with holders' digital identity wallets. Furthermore, depending on the role an organization takes in the digital identity ecosystem, these institutional wallets provide dedicated features for issuing and/or verifying digital attestations. Features for issuing attestations include applications that generate templates for digital attestations, convert identity information into digital attestations, and tools for digitally signing these. OpenID provides one emerging standard for related attestation issuing protocols for verifiable credentials (OID4VC) specifications (Chadwick and Vercammen, 2022). Moreover, institutional wallets allow issuers to revoke specific digital attestations when needed and publish related trusted revocation lists (Glöckler et al., 2023). Verifier tools, in turn, allow organizations to establish secure communication channels with the holders' digital identity wallet, generate proof requests, receive presentations, and connect to trust registries to verify these presentations.

Although digital services are becoming the "new normal," the use of decentralized digital identities and digital identity wallets shall not be limited to online interactions. Instead, emerging digital identity wallet solutions, such as the EUDIW, are designed to support both sharing digital attestations online and in face-to-face interactions. Yet, depending on the underlying use case, the holder's digital identity wallets and verifier tools may implement different standards that support the sharing of digital attestations in both online and offline scenarios. Prominent standards for the online sharing of digital attestations are the Open ID Connect for verifiable presentation (OIDC4VP) (Chadwick and Vercammen, 2022) and the self-issued OpenID provider (SIOP) (Yasuda et al., 2023) protocols. However, these protocols cannot be applied in offline (often also termed as face-to-face or proximity) interactions between holder and verifier. In such scenarios, digital identity wallets typically use near-field communication (NFC) or quick response (QR) codes to establish an initial connection and transfer a proof request. Once this initial communication has been established, digital attestations can be presented using NFC or QR codes or Bluetooth low energy (BLE) (ISO/IEC, 2021).

4.6 Trust Infrastructures

While PKC and digital signatures provide technical means for authenticating attestation issuers and verifiers, their effectiveness strongly depends on the available meta-information concerning who controls the respective cryptographic keypair. To this end, systems for managing decentralized digital identities deploy trust infrastructures (often also termed verifiable data registries, trust registries, or trusted lists) that provide required certified meta-information (Sedlmeir et al., 2021; Preukschat and Reed, 2021).

In more detail, trust infrastructures are typically employed as public key infrastructure (PKI) based on certificate authorities (CAs). That is, trust infrastructures serve as a registry for legal entities that distribute verifiable information on issuers and verifiers, such as their public keys and related metadata. This data can be used to verify the digital signature and authenticity of a digital attestation (Feulner et al., 2022). The information provided by trusted registries is not only beneficial for verifiers but can also prevent holders from sharing their personal information with malicious actors and being exposed to machine-in-the-middle (MITM) attacks (Babel and Sedlmeir, 2023). To this end, digital identity wallets can connect to the registry to identify the verifier based on its public key before establishing a secure connection and sharing any personal data.

Besides implementing registries for legal entities, trust infrastructures are also important for implementing attestation revocation mechanisms. They provide a mechanism to verify the current status of a presented attestation and ensure that any communication or transaction is based on valid and trustworthy information. A well-designed revocation registry should provide issuers with the means to publish efficient, scalable, privacy-preserving, and tamper-evident revocation status (Glöckler et al., 2023). Different approaches exist for the implementation of such revocation registries. For instance, downloadable revocation lists (e.g., certificate revocation list (CRL) enlist *all* attestations that are no longer valid by providing attestation identifiers, revocation date and time, revocation reason, and the issuer's signature. In contrast, the active 'phone home' (e.g., online certificate status protocol (OCSP) approach allows active querying of the revocation registry for the revocation status of a specific attestation. Both approaches operate via unique identifiers, which can potentially allow tracking by the operator of the revocation list. As a remedy, public revocation registries paired with ZKPs of inclusion or non-inclusion, as seen in Hyperledger Aries, are suggested. However, even this method encounters scalability challenges because of the necessity for extensive revocation lists, prompting the exploration of innovative, more scalable solutions.

In addition to providing cryptographic meta-data for attestation verification and counter-party authentication, trust infrastructures may also be used to facilitate the standardization and interoperability of digital attestations (Preukschat and Reed, 2021). In particular, attestation issuers, governance authorities, or standardization bodies can deploy a public registry to distribute schemas that provide information on the domain-specific data model and required attributes for specific attestations. These schemas may help verifiers to interpret digital attestations and the specific attested attributes therein. They further may act as a blueprint for other issuers that aim to issue similar attestations (Schlatt et al., 2022).

Many decentralized digital identity management implementations, such as the European self-sovereign identity framework (ESSIF) (European Blockain Services Infrastructure, 2023), or the United Kingdom (UK)'s National Health Service (NHS) staff passport (Lacity and Carmel, 2022), explore the potential of blockchain technology for their trust registries. Using blockchain for these registries is deemed particularly useful as it enables transparent, tamper-resistant, and distributed operation. Thus, in contrast to trust infrastructures that rely on centralized databases, blockchain technology enables the development of trusted registries that are not controlled by a single entity.

Concerning the implementation of trust infrastructures, particularly the role of blockchain technology within these, it is essential to note potential privacy risks that may arise when designed improperly (Rieger et al., 2021). In particular, the storage of holders' personal data, such as digital attestations and identifiers, and also their public keys, compromises holders' privacy, as it may allow for tracing and profiling (Sedlmeir et al., 2022a). When using blockchain as a trust infrastructure, the tamper-resistant storage of such information may also contradict privacy regulations, such as the EU's GDPR and the therein granted right to erasure (Rieger et al., 2019). Thus, decentralized identity management systems must ensure that trust infrastructures do not store any information about natural persons (Hoess et al., 2023; Rieger et al., 2022).

4.7 Challenges

Governments and service providers are heavily investing in deploying decentralized digital identities. Yet, several technical challenges will significantly impact the adoption of decentralized digital identity and the ability to meet the related expectations of more user-controlled and privacy-preserving digital identity management.

Privacy implications are a major concern for decentralized digital identities, which require protecting personal information. ZKPs are an important privacy-enhancing technology (PET) that enables individuals to present certain (partial) information without revealing the (full) information itself. ZKPs thereby minimize vulnerability to potential breaches and undue access (Babel and Sedlmeir, 2023). Despite the promise of ZKPs, they introduce complexities in implementation and computational demands. Thus, achieving a truly robust and efficient ZKP system without sacrificing privacy or functionality remains an intricate problem.

Another challenge is the binding of identity-related data to a digital identity wallet device, which raises concerns about losing access to the digital identity. This necessitates intricate wallet recovery mechanisms, such as recovery through encrypted cloud backups (Sellung and Kubach, 2023). In this scenario, users must retain a designated recovery key created during the backup time in a secure location such as a hardware device or written note. Loss of this key results in an inability to access the wallet backup. Implementing and managing recovery mechanisms presents a multi-layered challenge, balancing security, privacy, and accessibility while considering all the scenarios in which recovery may be required (Sedlmeir et al., 2022a; Anderson, 2011).

While decentralized digital identities receive substantial traction, interoperability presents a significant challenge for digital identity wallets and digital attestation specifications and implementations (Rieger et al., 2022). As various solutions emerge, ensuring they can interact smoothly becomes vital. Diverse implementations can lead to friction and fragmentation, hindering user experience and broad adoption (Schlatt et al., 2022). To navigate these challenges, regulations, and policies play a major role in shaping the adoption and standardization, necessitating a careful balance between decentralized identity principles and public interest. Moreover, there is a pressing need for maturing complementary technical standards, such as communication protocols and data formats, ensuring consistent communication across different platforms, vendors, and national borders. (Sedlmeir et al., 2022a)

Furthermore, the hardware components that locally protect secret keys to access the digital identity wallets pose unique challenges. Due to the immense diversity in the market, different hardware, such as smartcards (e.g., eSIM), secure elements (SE), and trusted execution environments (TEEs)), can lead to inconsistencies among implementations and their relative security level (Bastian et al., 2023). The functional inflexibility of such embedded hardware components limits the compatibility with more mature ZKPs technology and requires novel solutions for achieving data minimization (Babel and Sedlmeir, 2023). Moreover, different hardware technologies can leave the system susceptible to vulnerabilities such as side-channel attacks, posing additional challenges for hardware and firmware developers to ensure proper protection of key material storage and usage in a trusted environment. Moreover, with the growing trend by service providers (issuers and verifiers) of offloading computations to the cloud, ensuring the secure execution of sensitive operations in cloud-based TEEs becomes crucial, adding another layer of complexity to the intricate landscape of hardware security (Geppert et al., 2022).

Lastly, it is important to note that decentralized digital identity systems are not inherently secure. As they rely on common cryptographic algorithms such as Rivest-Shamir-Adleman (RSA) and ECC, decentralized digital identities are vulnerable to quantum attacks. Making such systems quantum secure requires moving to post-quantum cryptographic algorithms that are expected to resist quantum computing attacks, such as Kyber and Dilithium, which involve performances that are not fully standardized yet NIST (2017).

4.8 Conclusion

This chapter presented an introduction to the technical building blocks of a new identity management paradigm based on strong cryptographic foundations supporting trust infrastructures and digital attestations, stored in digital identity wallets controlled by the users themselves. As with any technology impacting existing ecosystems, challenges must be overcome to realize its full potential, with interoperability and recoverability of identity attestations being the most salient.

Decentralized Digital Identities will profoundly redefine the relationship between financial sector actors and their customers by transforming onboarding and authentication processes. New opportunities for the most innovative actors to provide new types of digital services through digital identity wallets will emerge, encompassing identity and communications capabilities. Standardized identity attribute provision mechanisms will enable them to more easily generate identity assurance for compliance purposes, while having the certainty that it is government certified, and thus reduce the administrative overhead associated with data management.

Despite the challenges ahead, powerful technology actors have already started building their identity wallets and providing services around them. For example, Apple now provides a wallet for digital driver's licenses in the United States of America (USA), and institutional actors are also currently preparing their large-scale introduction, such as the EUDIW. With these powerful institutional and economic actors committing to the technology, these challenges will eventually be solved, for decentralized digital identities to become a reality for service providers and users alike.

4.9 References

Allen, C. (2016). The path to self-sovereign identity http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Anderson, R. (2011). Can we fix the security economics of federated authentication? In *International Workshop on Security Protocols* (pp. 33–48).: Springer https://doi.org/10.1007/978-3-642-25867-1_5.

Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities. *European Business Organization Law Review*, *20*(1), 55–80, https://doi.org/10.1007/s40804-019-00135-1.

Babel, M. & Sedlmeir, J. (2023). Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs https://arxiv.org/abs/2301.00823.

Bastian, P., Kraus, M., & Fischer, J. (2023). Concepts for secure wallets in decentralized identity ecosystems. *HMD Praxis der Wirtschaftsinformatik*, *60*(2), 381–404, https://doi.org/10.1365/s40702-023-00954-4.

BSI (2023). Cryptographic mechanisms: Recommendations and key lengths https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html?nn=132646.

Cameron, K. (2005). The laws of identity https://www.identityblog.com/?p=352.

Chadwick, K. N. & Vercammen, J. (2022). OpenID for verifiable credentials https://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf.

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over IP stack. *IEEE Communications Standards Magazine*, *3*(4), 46–51, https://doi.org/10.1109/mcomstd.001.1900029.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*, 193–203, https://doi.org/10.1016/j.clsr.2017.10.003.

Diffie, W. & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6) https://doi.org/10.1145/3549993.3550007.

European Blockain Services Infrastructure (2023). Verifiable credentials framework https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/.

European Commission (2023). The European digital identity wallet architecture and reference framework https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

Fabcic, D. (2021). Strong customer authentication in online payments under GDPR and PSD2: A case of cumulative application. In *Privacy and Identity Management: IFIP Advances in Information and Communication Technology* (pp. 78–95). Springer https://doi.org/10.1007/978-3-030-72465-8_5.

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*, *32*, 1759–1777, https://doi.org/10.1007/s12525-022-00573-9.

Gaedke, M., Meinecke, J., & Nussbaumer, M. (2005). A modeling approach to federated identity and access management. In *14th International Conference on World Wide Web* (pp. 1156–1157). https://doi.org/10.1145/1062745.1062916.

Geppert, T., Deml, S., Sturzenegger, D., & Ebert, N. (2022). Trusted execution environments: Applications and organizational challenges. *Frontiers in Computer Science*, *4*, 930741, https://doi.org/10.3389/fcomp.2022.930741.

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*, https://doi.org/10.1007/s12599-023-00830-x.

Goldreich, O. & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, *7*(1), https://doi.org/10.1007/BF00195207.

Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept me as I am or see me go: A qualitative analysis of user acceptance of self-sovereign identity applications. In *Proceedings of the 56th Hawaii International Conference on System Sciences* (pp. 6560–6569). https://hdl.handle.net/10125/103427.

Hoess, A., Rieger, A., Roth, T., Fridgen, G., & Young, A. G. (2023). Managing fashionable organizing visions: Evidence from the european blockchain services infrastructure. In *Proceedings of the 31st European Conference on Information Systems*: AIS https://aisel.aisnet.org/ecis2023_rp/337/.

ISO/IEC (2021). ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application https://www.iso.org/standard/69084.html.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*.

Lacity, M. & Carmel, E. (2022). Implementing self-sovereign identity (SSI) for a digital staff passport at UK NHS. *University of Arkansas* https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2018/01/BCoE2022SS1FINAL.pdf.

Lacity, M., Carmel, E., Young, A. G., & Roth, T. (2023). The quiet corner of Web3 that means business. *MIT Sloan Management Review*, *64*(3) https://sloanreview.mit.edu/article/the-quiet-corner-of-web3-that-means-business/.

Luciano, D. & Prichett, G. (1987). Cryptology: From Caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, *18*(1), 2–17, https://doi.org/10.1080/07468342.1987.11973000.

Maler, E. & Reed, D. (2008). The Venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy*, *6*, 16–23, https://doi.org/10.1109/msp.2008.50.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86, https://doi.org/10.1016/j.cosrev.2018.10.002.

NIST, Computer Security Division, I. T. L. (2017). Post-quantum cryptography https://csrc.nist.gov/projects/post-quantum-cryptography.

Preukschat, A. & Reed, D. (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning Publications.

Richter, D., Praas, C. R., & Anke, J. (2023). Beyond paper and plastic: A meta-model for credential use and governance. In *Proceedings of the 31st European Conference on Information Systems*: AIS https://aisel.aisnet.org/ecis2023_rp/371/.

Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., & Fridgen, G. (2019). Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive*, *18*(4), 263–279, https://doi.org/10.17705/2msqe.00020.

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2021). The privacy challenge in the race for digital vaccination certificates. *Med*, *2*, 633–634, https://doi.org/10.1016/j.medj.2021.04.018.

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, *6*(1), 3–3, https://doi.org/10.1038/s41562-021-01243-0.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126, https://doi.org/10.1145/359340.359342.

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at first sight? A user experience study of self-sovereign identity wallets. In *Proceedings of the 30th European Conference on Information Systems*: AIS https://aisel.aisnet.org/ecis2022_rp/46/.

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, *59*(7), https://doi.org/10.1016/j.im.2021.103553.

Sedlmeir, J., Barbereau, T., Huber, J., Weigl, L., & Roth, T. (2022). Transition pathways towards design principles of self-sovereign identity. In *43rd International Conference on Information Systems*: AIS https://aisel.aisnet.org/icis2022/is_implement/is_implement/4/.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603–613, https://doi.org/10.1007/s12599-021-00722-y.

Sellung, R. & Kubach, M. (2023). Research on user experience for digital identity wallets: State-of-the-art and recommendations. In *Open Identity Summit* (pp. 39–50).: Gesellschaft für Informatik eV https://doi.org/10.18420/OID2023_03.

W3C (2023). Verifiable credentials data model 2.0 https://www.w3.org/TR/vc-data-model-2.0/.

Weigl, L., Amard, A., Codagnone, C., & Fridgen, G. (2023). The EU's digital identity policy: Tracing policy punctuations. In *15th International Conference on Theory and Practice of Electronic Governance* (pp. 74–81).: ACM https://dl.acm.org/doi/10.1145/3560107.3560121.

Weigl, L., Barbereau, T. J., Rieger, A., & Fridgen, G. (2022). The social construction of self-sovereign identity: An extended model of interpretive flexibility. In *Proceedings of the 55th Hawaii International Conference on System Sciences* (pp. 2543–2552). https://doi.org/10.24251/hicss.2022.316.

Yasuda, K., Loddersted, T., & Jones, M. (2023). Self-issued OpenID Provider v2 https://openid.net/specs/openid-connect-self-issued-v2-1_0.html.