z-Commerce: Designing a data-minimizing one-click checkout solution*

Egor Ermolaev[0000−0003−3412−5082]**, Iván Abellán Álvarez[0000−0003−4670−433X], Johannes Sedlmeir[0000−0003−2631−8749], and Gilbert Fridgen[0000−0001−7037−4807]

Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg
{egor.ermolaev,ivan.abellan,johannes.sedlmeir,gilbert.fridgen}@uni.lu
https://wwwen.uni.lu/snt/research/finatrax

Abstract. E-commerce has grown rapidly over the past years, with prevailing e-commerce platforms aggregating large amounts of customer data. This practice has several undesirable side effects, such as facilitating profiling that may lead to price discrimination and data feedback loops that can hamper competition. Moreover, data hoarding carries security risks through data breaches and undermines customers' privacy expectations. On the other hand, convenience aspects and compliance regulation demand the processing and storage of user-related data. To address this tension field, we aim to conceptualize and iteratively refine a data-minimizinig e-commerce platform. Following a design science research approach, we identify design objectives and propose and implement a solution in which stakeholders receive only customer data that is indispensable for their part of the process. Our solution leverages digital identity wallets and general-purpose zero-knowledge proofs (zk-SNARKs). We aim to perform a criteria-based evaluation to assess our artifact's feasibility and fitness from an interdisciplinary perspective. With our results, we hope to illustrate that combining state-of-the-art cryptographic techniques and an emerging digital identity paradigm allows reaching the user experience of incumbent e-commerce platforms while mitigating the undesirable socio-economic side effects of avoidable data disclosure.

Keywords: Compliance, digital wallet, electronic commerce, platform, selective disclosure, privacy, zero-knowledge proof

1 Introduction

Electronic markets facilitate the discovery and coordination of stakeholders such as buyers and sellers, data trading, product matching, and payments through

* This research was funded in part by the Luxembourg National Research Fund (FNR) through the PABLO project (grant reference 16326754) and by PayPal, grant reference "P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen" (PEARL).

** Corresponding author (e-mail: egor.ermolaev@uni.lu)

digital means [56]. E-commerce is seen as a shift from traditional markets into the digital economy [40]. Corresponding digital platforms use digital technologies to fulfill business and market requirements, yet may also involve physical processes, for instance, for product delivery. E-commerce offers several benefits to merchants and consumers. First, the digital coordination of purchase-related processes, such as business-to-consumer interactions during payment and delivery, makes the corresponding markets ubiquitous [57] and more efficient, especially at large distances. Second, a single integrated platform, among other benefits, enables customers to efficiently discover products or services [65]. Third, e-commerce facilitates delivery based on customer preferences, such as shipment to door, to pick-up points, or just to the closest post office. It thus improves distant goods distribution [43] and benefits customers who would be limited to local sellers with a limited spectrum of available products. Fourth, e-commerce improves user experience by facilitating remote purchase agreements with integrated electronic payments [47]. Studies suggest that in 2022, e-commerce accounted for more than 5 trillion U.S. dollars in retail sales [35] and that e-commerce sales may further increase substantially over the next few years. Particularly large e-commerce platforms such as Amazon have grown enormously. This can be attributed to the presence of indirect network effects, as platforms with the greatest selection of merchants and their goods provide the highest utility to consumers and vice versa [4].

1.1 Benefits of data collection

Data processing is a key aspect of e-commerce due to multiple business requirements that include accounting, legal, recommender systems, and payment processing activities [47]. For instance, a legal requirement would be an age verification for purchasing alcohol, whereas a business requirement could be the disclosure of the residential address for product delivery. In this context, a user first obtains a user account on the e-commerce website by providing personal information. A registration process is not only used by merchants but also underlies payment, as banks or payment service providers (PSPs) need to conduct know-your-customer (KYC) processes based on verifiable personal data retrieved, for instance, from a national ID card [53]. As the registration process is time-consuming for the user and the verification of identity attributes may also be costly for the vendor, e-commerce providers store their customers' identity attributes to have them available for subsequent interactions. At the checkout process, platforms then ensure account ownership via authenticating their users [58]; typically using passwords and potentially additional factors. The inconvenience of registering with multiple service providers by filling out forms not only in e-commerce but also beyond has led to the appearance of identity providers (IdPs) who centrally collect users' identity information to offer single sign-on solutions [54]. To improve user experience, many e-commerce platforms and also independent merchants have integrated this federated identity model to allow users to authenticate with an existing account with their IdP and to transfer corresponding identity attributes without the need for repeated

registration [31]. For instance, Amazon already acts as an IdP for many small vendors to provide their users with a one-click checkout without prior registration, and, thereby, extends its data collection even beyond consumers on its own e-commerce platform.

Data collection also benefits e-commerce platforms beyond improving user experience in the context of identity management. Targeted advertising to promote products is key in the e-commerce business model [3,7]. Recommender systems attract customers by advertising those offers that customers may be most interested in [65]. Personalized product recommendation is known to increase sales [66], which represents a major driver to improve the corresponding recommendation systems, for example, by training machine learning models on collected transaction data [66]. E-commerce platforms that aggregate multiple retail stores and small-sized merchants can, therefore, improve their service and provide more convenience to customers [40]. Data collection also improves the effectiveness of e-commerce platforms toward customer relationships [39]. Customer data gathering helps to tailor relationship management, for example, by making advertising campaigns more compelling, introducing effective customer retention techniques such as loyalty programs, or improving service quality to meet customers' expectations [39].

1.2 Problems in the context of data collection

On the other hand, data collection through e-commerce platforms carries several economic, security, and privacy risks. Large-scale data collection allows for profiling customers, i.e., analyzing their transaction histories and modeling their behavior [34]. This profiling may lead to unfair treatment of customers, such as price discrimination [11]. Moreover, indirect network effects and the corresponding accumulation of market power to large e-commerce platforms are further increased: Direct access to customers' data may make dominant platforms feel tempted to practice anti-competitive measures, for instance, by placing lock-in practices through making data non-portable [15]. Additionally, platforms can also benefit from data feedback loops [29] and data network effects [25], so they could gain market share as advanced data analytics allows them to improve faster. Likewise, these marketplace aggregators, which offer convenience to both retailers and customers, can exploit other revenue streams, such as charging membership, service, or commission fees [40], allowing them to reduce fees and make them more attractive. All these practices significantly increase the market power of large, incumbent e-commerce platforms, ultimately hampering competition [29]. Additionally, collected data is generally stored in centralized silos [12], facing risk of being harvested without users' explicit consent [63]. As such, users have little control over whether their data is being sold to third parties [21]. Moreover, insufficient security measures or targeted attacks on "honey pots" can lead to data leaks or breaches. For instance, a hacker's raid on eBay led to a historic breach that leaked 145M user records in 2014 [48]. It is not only that data breaches pose a risk to privacy, as sensitive information may be exposed to third parties without consent. They also represent a substantial security threat,

as users may be targeted for impersonation or social engineering attacks where publicly available information is exploited for malicious purposes [38]. Opaque data flows, advanced data analytics, and transaction monitoring also raise concerns among users who dislike disclosing personal information [39] or who fear the implementation of surveillance capitalism or an Orwellian state [67].

1.3 Searching for new solutions

We conclude that the handling and processing of customer data need to navigate between convenience and business requirements on the one hand and security, privacy, and socio-economic risks on the other hand. Balancing users' privacy and business and compliance needs that require data collection is already a problem without an easy solution in electronic payments alone [41]. Arguably, balancing out this tension field in e-commerce may be even more challenging as it involves further business and compliance requirements, more complex processes, and additional stakeholders guided by their own interests. Some regulations and initiatives aim to address selected issues; for instance, the general data protection regulation (GDPR) aims to ensure the good and appropriate management of European citizens' personal data [62]. The Payment Services Directive (PSD2) enforces information security of payments conducted by financial institutions and PSPs [18]. Most recently, the Digital Services Act (DSA) introduced a set of measures to protect customer rights and ensure an accountable and fair competitive digital market, targeting "gatekeepers" that include e-commerce platforms such as Amazon [19]. Privacy-enhancing technologies have been proposed also in related areas, such as data markets for the Internet of Things (IoT) [22].

New trends in digital identity and privacy-enhancing technology, such as zero-knowledge proofs (ZKPs), may help pave the way toward convenient and yet privacy-oriented e-commerce solutions. In this paper, we investigate to which extent recent approaches to privacy-oriented digital interactions in the realm of identification [50,54] and payments [17,26,64] can be used for this purpose. Researchers have consistently encouraged the use of cryptography in this context [16,49], and corresponding solutions are increasingly discussed and explored [26,61]. Many approaches rely on ZKPs to facilitate the convenient, selective disclosure of information from users to relying parties, such as digital platforms, service providers, or blockchain-based applications, in a machine-verifiable way. For instance, requirements of an e-commerce transaction from a regulatory or business side should be verified effectively while reducing the processing of sensitive information to a minimum.

However, there has only been limited research on combining such tools in practical applications, particularly in the context of e-commerce. In contrast, most prior research has focused either on exchanging only identity-related data for specific business or administrative processes or on privacy-oriented payments but not on their combination. The work by Schanzenbach et al. [52] poses a notable exception that implements both decentralized identity management and a client-side payment system for e-commerce. However, it has a strong technical perspective, is subject to several limitations, and lacks consideration of how to

coordinate the different stakeholders involved in an e-commerce purchase process. Related work has also not evaluated a data-minimal e-commerce (DMEC) solution with regard to stakeholders' expectations. We believe that the case of e-commerce may indeed illustrate the impact of novel data-minimizing technologies from an individual, economic, and societal perspective, combining both user and business perspectives. Integrating a corresponding wide variety of privacy features in a digital wallet may provide an alternative, "one-click registration and checkout" process that avoids unnecessary data processing and storage while maintaining a high level of user experience [32,51,28]. This direction could also shed light on new directions to preventing the privacy paradox [1].

Our work hence designs and evaluates a proof-of-concept that an alternative, data-minimizing approach to e-commerce is possible. Our system facilitates the selective disclosure of personal and payment information to stakeholders involved in a transaction on an e-commerce platform. We follow the design science research (DSR) methodology by Peffers et al. [45] to develop an artifact that addresses both users' and businesses' needs in the tension field between data use and data minimization. With our artifact, we aim to provide design knowledge on how to build data-minimizing e-commerce solutions. We plan to evaluate the artifact from an interdisciplinary perspective to demonstrate the feasibility and suitability of using digital wallets and ZKPs for achieving minimal information disclosure in e-commerce.

The remainder of this paper is structured as follows: In Section 2, we introduce background knowledge on ZKPs and where they are currently explored in practice in the form of privacy-oriented digital identity management and payments. We then review related work on privacy-oriented e-commerce solutions. Section 3 presents how we aim to conduct our design science research approach in detail and how we believe our research can contribute to the information systems domain.

2 Background and Related Work

2.1 Foundational building blocks

Zero-knowledge proofs: Goldwasser et al. [23] introduced the notion of zero-knowledge in interactive proof systems. It is a property of an interaction between two subjects, a "prover" and a "verifier". The prover probabilistically convinces the verifier of a statement while revealing no additional information about why the statement is true. For instance, the prover could convince the verifier that she knows a solution to a given Sudoku puzzle, without revealing any field of the solution to the verifier. The probability of a malicious prover convincing the verifier of a wrong statement decreases exponentially in the number of interactions between the prover and the verifier. Zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK) are a family of ZKP that eliminates the need for interactions between the prover and the verifier by obtaining randomness using cryptography. zk-SNARKs also satisfy an additional property that makes them extremely efficient from the perspective of the verifier: They are succinct,

i.e., the resulting proof is very short, and its verification is much quicker than verifying the statement directly through naive re-computation [27]. General-purpose zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) have rapidly evolved during the last few years because of their natural fit for solving technical challenges related to blockchain technology [55,9], with emerging domain-specific languages (DSLs) (e.g., Circom, ZoKrates), libraries (e.g. Circomlib) and tools (e.g. SnarkJS) that allow software engineers to implement ZKPs for a broad class of statements. This development has accelerated research and application of zero-knowledge technology also beyond blockchains, such as in digital identity [6], payment systems [26], and supply chains [42].

Digital identity: Decentralized or self-sovereign identity (SSI) is a concept that involves representing and sharing attributes or authorizations of individuals or organizations, with the aim of providing a more convenient alternative to traditional IdPs while empowering individuals to control data disclosure using digital wallets. SSI's core principles were first described by Allen [2] and later extended with insights from practical experiences [54]. They include not only user-centric requirements such as convenience aspects, control, and data-minimization but also organizational requirements, such as verifiability and authenticity. For instance, a notable application of ZKP is "anonymous credentials" [14] in the realm of digital identity. A prover can ensure a verifier about adulthood without disclosing the date of birth registered in his digital identity by means of a digitally signed ID card issued, for instance, by a national institution [54]. In this context, ZKPs guarantee the verifiability of selectively disclosed attributes, although the underlying digitally signed attestation is never shared. Thereby, ZKPs can be used for selective disclosure – "the ability of an individual to granularly decide what information to share" [60] – and privacy-by-design solutions. A popular implementation is Hyperledger Aries, which presents one of the first efforts for technical specifications and implementation of SSI using blockchain technology [53]. It uses Hyperledger AnonCreds, a library, and specification of anonymous credentials conceptualized by Camenisch & Lysyanskaya [14] that facilitate advanced privacy features such as the selective disclosure of attributes and the avoidance of unique identifiers using special purpose ZKPs. Several public and private sector projects, such as the public-private consortium IDunion, use Hyperledger Aries to implement a SSI-based digital identity management solution that addresses businesses' needs and that is compliant with the EU GDPR [5]. Recently, ZKPs are discussed in the context of the revision of the electronic IDentification, Authentication and trust Services (eIDAS) regulation[13]. These and similar designs support limited functionalities due to the cryptographic primitives they use [6]. However, using these components in the context of e-commerce requires support for adoption at a large scale and more flexible and sophisticated predicates. Therefore, new research focuses on extending the data minimization capabilities of anonymous credentials using general-purpose ZKPs. For instance, several works including [50] and [6] adopt zk-SNARKs to prove complex composable statements about identity attributes without disclosing the signed attestation and to address some scalability shortcomings of the AnonCreds implementation.

Payment systems represent an essential component of e-commerce. Cash is not sufficient for e-commerce due to limitations regarding convenience, such as remote purchasing, and security requirements for a safe transfer. Therefore, electronic payment systems seem more suitable. During the payment process, customers then need to reveal sensitive information to address compliance, technical, and processing requirements to their PSPs. Consequently, PSPs typically have access to transaction data and history. Also, the approach of sharing credit card information with the merchant, including legal name, credit card number, and security code, allows for transaction traceability and is far from data minimizing. To address privacy concerns in electronic payments. Chaum [16] introduced "e-cash" using blind signatures, which provides privacy to the payer. This solution is not flexible enough as the payee is fully transparent. ZeroCash [10] describes a completely anonymous digital currency leveraging ZKP. However, these approaches to anonymous payments do not comply with money laundering and terrorist financing regulation [26]. GNU Taler [17], another implementation of privacy-oriented payment systems based on Chaum's initial e-cash approach, addresses compliance issues by introducing the "auditor" role to which both users and payment processors are accountable. It provides a privacy-friendly payment system solution for the payer, who remains anonymous. Several recent works present alternative centralized or decentralized payment systems to address both privacy demands and compliance by enforcing turnover limits for anonymous transactions [26,64]. These architectures can be considered the next iteration of privacy-focused, ZKPs and blockchain-based cryptocurrencies such as Zcash [10] that in contrast have a solid chance of achieving regulatory compliance.

2.2 Related work

Data markets: DISSENS [52] provides decentralized identity management and a client-side payment system for e-commerce. It aims to be a regulatory-compliant solution built on a decentralized network, specifically a distributed hash table (DHT), that acts as an encrypted file storage for digital identity. Integrating the GNU Taler [17] payment system ensures client-side privacy features and provable regulatory compliance. However, several limitations prevail. Data, although encrypted, is shared on a public network, which may conflict with the GDPR's "right to be forgotten". Its functionality is limited to the disclosed attributes, so extensive functionality is not possible, such that proving general statements concerning one or multiple attributes. Agora [37] proposes a semi-private marketplace for data brokerage. Users generate encrypted data which upon payment brokers decrypt and batch. Brokers act as an unlinkability and aggregator service to interested data buyers, thus protecting users' data in front of end consumers. Due to the nature of the cryptographic algorithms used, their cryptographic protocols are limited in functionality. Agora only supports private data sharing of special mathematical function outputs, such as weighted averages and linear regressions. The paper highlights that functionality could

be improved by leveraging ZKP. For instance, Garrido et al. [22] survey different privacy-enhancing technologies (PETs) in IoT data markets and illustrate their trade-offs. Data brokerage may use various PETs to enable aggregation and obfuscation of the initial private data that makes it irreversible and untraceable. Similarly, a centralized approach is proposed for data collection and service delivery [44]. Data generators use a particular cryptographic primitive to protect and preserve privacy by computing encrypted data. However, the system relies on a third party to create participants' identities, which may pose a risk to data privacy guarantees. If eventually, the registration center becomes corrupted, it could intercept and decrypt the data, thus correlating users to content. Additionally, a tamper-proof device is required, which usually poses an encumbrance to widespread adoption. Bella et al. [8] suggests an e-commerce architecture that balances privacy and trust by using differential privacy. Differential privacy introduces noise to make user data less sensitive, which brings fuzziness to the characteristics of each customer (e.g., adulthood). Hence, differential privacy approaches may not be adequate, particularly when clear boundaries are imposed by regulatory compliance considerations.

Besides some technical limitations of related work that we aim to address, we also note that related work, except for DISSENS [52], so far has not evaluated their solutions with stakeholders, for instance, to assess whether the approach can meet business needs and customers' user experience needs.

3 Method

In this paper, we outline how we aim to create general prescriptive knowledge on reducing the processing and storage of sensitive information in e-commerce following the DSR method [45]. Based on a demonstration of the feasibility of such a design, we want to identify how this approach can help avoid the aggregation of data by incumbent e-commerce platforms and the corresponding security and socio-economic challenges we discussed in Section 1. Our research hence provides an interdisciplinary perspective from an information systems lens by developing a solution based on novel cryptographic tools. Our research also addresses calls for more widespread applications of cryptography for "moral" reasons, for instance, to tackle increasing surveillance threats [49].

Our paper is structured according to the DSR best practices as described by Gregor & Hevner [24], yet considers the limitation of our paper's scope as it represents research in progress. We first comprehensively identify the problem and motivation. A valuable DSR artifact must satisfy a certain societal or business need [30] to determine the relevance and value of the contribution to the IS research field. According to Section 1, the accumulation of customer data and the corresponding economic implications (e.g., opportunities for price discrimination based on customer profiling and negative consequences for competition through data feedback loops), security threats, and moral issues pose such a need [49]. We aim to ensure both the relevance of our research and the fitness of our artifact by first more clearly identifying the research problem, identifying the

roles, tasks, and requirements of the relevant stakeholders in a systematic literature review, and deriving comprehensive objectives of the solution in the future. As we argued in Section 1, the objectives will involve convenience expectations regarding end-user experience, regulatory compliance, and data minimization. We plan to validate and potentially extend these requirements based on expert interviews during the first evaluation cycle of our DSR. We plan to apply the convenience sampling method for interviews. We will form groups of interviewees with respect to their domain of expertise and involve also end-users to have a balanced sample. The selection criteria will correspond to the domains involved in our research, such as cryptographers or IT security researchers, and experts from the business side on e-commerce and adjacent service providers, such as logistics.

We follow the design science research methodology (DSRM) proposed by Peffers et al. [45]. Fig. 1 features the corresponding iterative build-and-evaluation cycles. We aim to design and develop our artifact – a DMEC architecture and corresponding information flow that only shares and stores information that is indispensable for each stakeholder and, therefore, mitigates undesirable side effects such as price discrimination against consumers and accumulation of market power. The design will also define onboarding and end-to-end purchasing processes for customers. The build-and-evaluate process is at the core of DSR and helps IS researchers discover answers to problems that have not been resolved before [30]. The DSR method emerged to combine methods from engineering and social sciences for practically relevant, rigorous research [24]. Thus, one can apply the DSR approach to a broad spectrum of domains. The design of a DMEC platform addresses the tension field between convenience, compliance, and data minimization and, therefore, affects both technical and non-technical considerations that need to be incorporated in the development from an engineering and social sciences perspective. Yet, we believe that the implications of our DSR go far beyond e-commerce and may be applicable to adjacent realms such as e-government [20], healthcare [33], the industrial IoT [59], which also seem to involve tensions between data sharing needs and data protection considerations. Particularly blockchain-based applications require such data minimization by design owing to the inherent transparency of distributed ledgers [55,46].

During the process iterations of the DSRM process model, we also instantiate our artifact in the form of a prototype based on the architecture. We will use this instantiation both for the first set of more technical design iterations and for demonstration in the interview-based evaluation. For preparing the implementation, we will define the components of the high-level system architecture and their functionality. Then we will search for potential open-source solutions which can be used in the components. Particularly, we will analyze which open-source solutions could help us to implement the ZKP stack that provides selective disclosure. There will be multiple criteria for ZKP stack selection, such as the performance of proof generation (especially when considering a prototype for e-commerce on mobile devices). So far, we have closely analyzed several promising

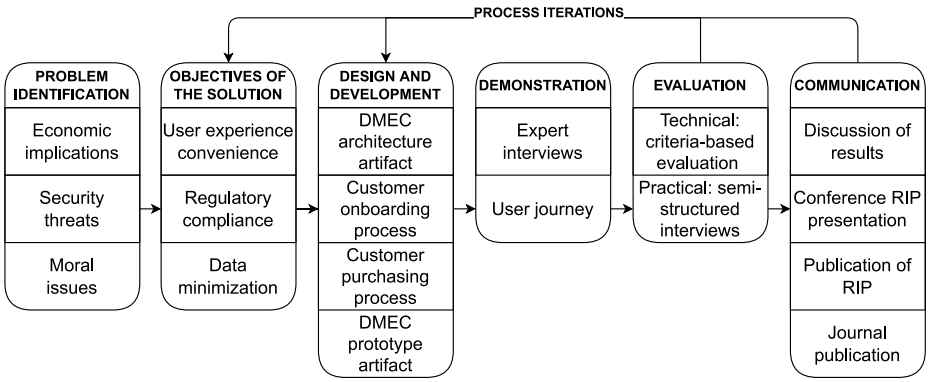

Fig. 1. Our applied DSR approach to design a DMEC architecture following Peffers et al. [45].

open-source solutions as candidates and assessed their potential extension for the needs of our architecture.

The Heimdall framework [6] promises a good fit for our technical requirements. As we highlighted in Section 2, related work on privacy-oriented e-commerce solutions still lacks essential features. The Heimdall framework provides several of these features as it implements anonymous credentials that facilitate seamlessly and verifiably sharing the minimum identity-related data required by the relying party in a scalable way [6]. In particular, Heimdall provides a modular set of tools to create, issue, verify, and manage verifiable credentials. Concretely, the framework supports "prover" and "verifier" functions. Users are able to manage and store issued verifiable credentials. They are also capable of generating data minimizing presentations upon verifiers' request in a private way (e.g., selectively disclosing personal information). They do so by means of ZKP, in particular zk-SNARK. Nonetheless, we envision the need to extend Heimdall's functionality to make it compatible with all the project's needs, which is feasible because zk-SNARKs are general-purpose and can be used to prove any statement. The envisioned artifact is in the form of an e-commerce architecture consisting of four main components, namely a checkout page, a digital identity wallet, a back-end architecture, and an agent. The checkout page implements potential checkout options of an e-commerce platform. The digital identity wallet, in which the customer manages identities, serves as a wallet application to share the minimal necessary information with the merchant. When customers indicate their intention to purchase through the website, this communicates with the e-commerce back-end so that the agent establishes a connection with the digital identity wallet. Customers are then able to generate proofs, which are based on the credentials stored in the wallet, in response to the agent's request. The agent verifies and confirms the user-generated proof and sends the appropriate user data to the checkout page.

During the iterations, we will synchronize the evolved design of the system architecture and development direction. The iterations will go in parallel for all the artifacts: the design, processes, and prototype. At the end of each iteration, the quality of the artifacts will be evaluated both technically (performance benchmarking, as mentioned before) and practically (interviews with relevant stakeholders). For demonstration and continuous improvement, we will conduct multiple interview cycles and evaluate user journeys with groups of people, which will contribute to the design and development as part of the process iterations by disseminating the intermediate progress with the stakeholders and receiving their feedback. Interviews will be essential for collecting feedback regarding the practical side of the prototype to evaluate user experience. There are only a few studies on how users experience the use of digital wallets, particularly data minimization capabilities [51,36], and we believe that presenting users with a familiar flow, such as commerce, may help gain new insights. The collected feedback will also be implemented according to the DSRM process model.

The envisioned artifact is in the form of an e-commerce architecture consisting of four main components, namely a checkout page, a digital identity wallet, a back-end architecture (controller), and an agent. The checkout page implements a checkout option – "checkout with SSI". The digital identity wallet allows customers to share the minimal identity information necessary with the merchant and other stakeholders, such as logistics service providers. We will use the design tools for layouts of both front-end components (checkout page and wallet). When a customer indicates their intention to purchase through the website, the checkout page communicates with the merchant back-end so that the agent establishes a connection with the digital identity wallet and sends a proof request to it. Upon the customer's confirmation, the wallet generates a corresponding cryptographic proof (SNARK) based on the credentials stored in the wallet that addresses the agent request and sends it back to the verifying component of the agent. The agent cryptographically verifies the proof and notifies the merchant's back-end, which transmits the verified identity attributes to the checkout page for a corresponding user.

At the evaluation stage, we will validate the objectives of the solution by means of criteria-based evaluation and semi-structured interviews with stakeholders from both interdisciplinary and specific domains (e.g., business, law, user experience, and software engineering). We also plan to conduct user experience evaluations with our stakeholders. From the business-related interviews, we also aim to investigate the business opportunities of such a solution. At the communications stage, we will focus on the presentation and discussion of the research-in-progress paper at the conference. The second stage would be to publish the full paper. In the end, we will open-source the code of our prototype on GitHub.

4 Conclusion

The increasing market growth of e-commerce has led to the aggregation of large amounts of customer data. With the proliferation of incidents related to sensitive data breaches and abuses, both users and regulators are taking steps to protect privacy rights. In this light, we follow the design science research methodology according to Peffers et al. [45] to identify the feasibility of an e-commerce solution that addresses the tension field between convenience aspects and compliance regulation demand the processing and storage of user-related data. Following DSRM, we aim to derive the system architecture of DMEC and build a corresponding prototype. Our proposed solution utilizes digital identities and zero-knowledge proof as core components for privacy-oriented e-commerce transactions. Using an interdisciplinary, criteria-based evaluation, we aim to demonstrate that our artifact can address the societal and business needs that we previously discussed and serve as a starting point for many relevant studies in information systems on usable privacy.

References

1. Alashoor, T., Keil, M., Smith, H.J., McConnell, A.R.: Too tired and in too good of a mood to worry about privacy: Explaining the privacy paradox through the lens of effort level in information processing. Information Systems Research (2022)
2. Allen, C.: The path to self-sovereign identity (2016), http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
3. Alt, R.: Electronic markets on business model development. Electronic Markets **30**(3), 405–411 (2020)
4. Alt, R.: Electronic markets on platform transformation. Electronic Markets **32**(2), 401–409 (2022)
5. Anke, J., Richter, D.: Digitale identitäten. HMD Praxis der Wirtschaftsinformatik (2023)
6. Babel, M., Sedlmeir, J.: Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs (2023), http://arxiv.org/abs/2301.00823
7. Baethge, C., Klier, J., Klier, M.: Social commerce – state-of-the-art and future research directions. Electronic Markets **26**(3), 269–290 (2016)
8. Bella, G., Giustolisi, R., Riccobene, S.: Enforcing privacy in e-commerce by balancing anonymity and trust. Computers & Security **30**(8), 705–718 (2011)
9. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity (2018), https://eprint.iacr.org/2018/046
10. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from Bitcoin. In: Proceedings of the IEEE Symposium on Security and Privacy. pp. 459–474 (2014)
11. Bergemann, D., Brooks, B., Morris, S.: The limits of price discrimination. American Economic Review **105**(3), 921–57 (2015)
12. Braud, A., Fromentoux, G., Radier, B., Le Grand, O.: The road to European digital sovereignty with Gaia-X and IDSA. IEEE Network **35**(2), 4–5 (2021)

13. Busch, C.: eidas 2.0: Digital identity service in platform economy (2022), https://cerre.eu/wp-content/uploads/2022/10/CERRE_Digital-Identity_Issue-Paper_FINAL-2.pdf
14. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. pp. 93–118 (2001)
15. Camp, L.J., Osorio, C.A.: Privacy-enhancing technologies for internet commerce (2002), https://papers.ssrn.com/abstract=329282
16. Chaum, D.: Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM **28**(10), 1030–1044 (1985)
17. Dold, F.: The GNU Taler system: Practical and provably secure electronic payments (2019), https://syntheses.univ-rennes1.fr/search-theses/notice.html?id=rennes1-ori-wf-1-12183&printable=true
18. European Central Bank: The revised payment services directive (PSD2) (2018), https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
19. European Comission: The digital services act: Ensuring a safe and accountable online environment (2022), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en
20. Fedorowicz, J., Gogan, J.L., Culnan, M.J.: Barriers to interorganizational information sharing in e-government: A stakeholder analysis. The Information Society **26**(5), 315–329 (2010)
21. Fienberg, S.E.: Privacy and confidentiality in an e-commerce world: Data mining, data warehousing, matching and disclosure limitation. Statistical Science **21**(2), 143–154 (2006)
22. Garrido, G.M., Sedlmeir, J., Uludağ, Ö., Alaoui, I.S., Luckow, A., Matthes, F.: 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 (2022)
23. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM Journal on Computing **18**(1), 186–208 (1989)
24. Gregor, S., Hevner, A.R.: Positioning and presenting design science research for maximum impact. MIS Quarterly **37**(2), 337–355 (2013)
25. Gregory, R.W., Henfridsson, O., Kaganer, E., Kyriakou, H.: The role of artificial intelligence and data network effects for creating user value. Academy of Management Review **46**(3), 534–551 (2021)
26. Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., Schellinger, B.: Designing a central bank digital currency with support for cash-like privacy (2021), https://papers.ssrn.com/abstract=3891121
27. Groth, J.: On the size of pairing-based non-interactive arguments. In: Advances in Cryptology – EUROCRYPT, pp. 305–326. Springer (2016)
28. Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., Zwede, T.: 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 (2023)
29. Hermes, S., Kaufmann-Ludwig, J., Schreieck, M.: A taxonomy of platform envelopment: Revealing patterns and particularities. In: Proceedings of the 26th Americas Conference on Information Systems (2020)

30. Hevner, A., March, S.T., Park, J., Ram, S., et al.: Design science research in information systems. MIS Quarterly **28**(1), 75–105 (2004)
31. Jøsang, A., Fabre, J., Hay, B., Dalziel, J., Pope, S.: Trust requirements in identity management. In: Proceedings of the 44th Australasian Workshop on Grid Computing and e-Research. pp. 99–108 (2005)
32. Jørgensen, K.P., Beck, R.: Universal wallets. Business & Information Systems Engineering **64**(1), 115–125 (2022)
33. Kaye, J.: The tension between data sharing and the protection of privacy in genomics research. Annual Review of Genomics and Human Genetics **13**(1), 415–431 (2012)
34. Kayes, I., Iamnitchi, A.: Privacy and security in online social networks: A survey. Online Social Networks and Media **3–4** (2017)
35. Keenan, M.: Global e-commerce: stats and trends to watch (2022), `https://www.shopify.com/enterprise/global-ecommerce-statistics`
36. Khayretdinova, A., Kubach, M., Sellung, R., Roßnagel, H.: Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In: Selbstbestimmung, Privatheit und Datenschutz : Gestaltungsoptionen für einen europäischen Weg, pp. 389–406. Springer Fachmedien Wiesbaden (2022)
37. Koutsos, V., Papadopoulos, D., Chatzopoulos, D., Tarkoma, S., Hui, P.: Agora: A privacy-aware data marketplace. IEEE Transactions on Dependable and Secure Computing **19**(6), 3728–3740 (2022)
38. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. Journal of Information Security and Applications **22**, 113–122 (2015)
39. Kumar, V., Reinartz, W.: Customer privacy concerns and privacy protective responses. In: Customer Relationship Management, pp. 285–309. Springer (2018)
40. Lee, C.: An analytical framework for evaluating e-commerce business models and strategies. Internet Research **11**(4), 349–359 (2001)
41. Maseeh, H.I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., Ashaduzzaman, M.: Privacy concerns in e-commerce: A multilevel meta-analysis. Psychology & Marketing **38**(10), 1779–1798 (2021)
42. Mattke, J., Maier, C., Hund, A.: How an enterprise blockchain application in the U.S. pharmaceuticals supply chain is saving lives. MIS Quarterly Executive **18**(4), 246–261 (2019)
43. Morganti, E., Seidel, S., Blanquart, C., Dablanc, L., Lenz, B.: The impact of e-commerce on final deliveries: Alternative parcel delivery services in France and Germany. Transportation Research Procedia **4**, 178–190 (2014)
44. Niu, C., Zheng, Z., Wu, F., Gao, X., Chen, G.: Achieving data truthfulness and privacy preservation in data markets'. IEEE Transactions on Knowledge and Data Engineering **31**(1), 105–119 (2019)
45. 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)
46. Platt, M., Bandara, R.J., Drăgnoiu, A.E., Krishnamoorthy, S.: Information privacy in decentralized applications. In: Trust Models for Next-Generation Blockchain Ecosystems, pp. 85–104. Springer (2021)
47. Qin, Z.: Introduction to e-commerce. Springer (2009)
48. Reuters, CNBC: Hackers raid eBay in historic breach, access 145M records (2014), `https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html`
49. Rogaway, P.: The moral character of cryptographic work (2015), `https://eprint.iacr.org/2015/1162`

50. Rosenberg, M., White, J., Garman, C., Miers, I.: zk-creds: Flexible anonymous credentials from zkSNARKs and existing identity infrastructure (2022), https://eprint.iacr.org/2022/878
51. Sartor, S., Sedlmeir, J., Rieger, A., Roth, T.: Love at first sight? A user experience study of self-sovereign identity wallets. In: Proceedings of 30th European Conference on Information Systems (2022)
52. Schanzenbach, M., Grothoff, C., Wenger, H., Kaul, M.: Decentralized identities for self-sovereign end-users (DISSENS). In: Proceedings of Open Identity Summit. pp. 47–58 (2021)
53. Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N.: Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management **59**(7), 103553 (2022)
54. Sedlmeir, J., Huber, J., Barbereau, T., Weigl, L., Roth, T.: Transition pathways towards design principles of self-sovereign identity. In: Proceedings of the 43rd International Conference on Information Systems (2022)
55. Sedlmeir, J., Lautenschlager, J., Fridgen, G., Urbach, N.: The transparency challenge of blockchain in organizations. Electronic Markets **32**, 1779–1794 (2022)
56. Stahl, F., Schomm, F., Vossen, G., Vomfell, L.: A classification framework for data marketplaces. Vietnam Journal of Computer Science **3**(3), 137–143 (2016)
57. Targett, D.: B2B or not B2B? Scenarios for the future of e-commerce. European Business Journal **13**(1) (2001)
58. Trautman, L.J.: E-commerce, cyber, and electronic payment system risks: Lessons from PayPal (2016), https://papers.ssrn.com/abstract=2314119
59. Ukil, A., Bandyopadhyay, S., Pal, A.: IoT-privacy: To be private or not to be private. In: Proceedings of the Conference on Computer Communications Workshops. pp. 123–124 (2014)
60. W3C: Engineering privacy for verified credentials (2022), https://w3c-ccg.github.io/data-minimization/#selective-disclosure
61. Weigl, L., Barbereau, T.J., Rieger, A., Fridgen, G.: 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 (2022)
62. Wolford, B.: What is GDPR, the EU's new data protection law? (2018), https://gdpr.eu/what-is-gdpr/
63. van der Wolk, A., Silva, K.: Insight: A slap on the wrist or show of force – GDPR fines reveal need for EU penalty guidelines (2019), https://news.bloomberglaw.com/privacy-and-data-security/insight-a-slap-on-the-wrist-or-show-of-force-gdpr-fines-reveal-need-for-eu-penalty-guidelines
64. Wüst, K., Kostiainen, K., Delius, N., Capkun, S.: Platypus: A central bank digital currency with unlinkable transactions and privacy-preserving regulation. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. pp. 2947–2960 (2022)
65. Youlong Zhuang, Albert L. Lederer: An instrument for measuring the business benefits of e-commerce retailing. International Journal of Electronic Commerce **7**(3), 65–99 (2003)
66. Zhou, L.: Product advertising recommendation in e-commerce based on deep learning and distributed expression. Electronic Commerce Research **20**(2), 321–342 (2020)
67. Zuboff, S.: Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology **30**(1), 75–89 (2015)