A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity

Johannes Sedlmeir, Jana Glöckler, Muriel-Larissa Frank, Gilbert Fridgen

Business & Information Systems Engineering (2023)

Appendix (available online via http://link.springer.com)

Appendix

A Systematic Literature Review

A.1 Relevant Articles

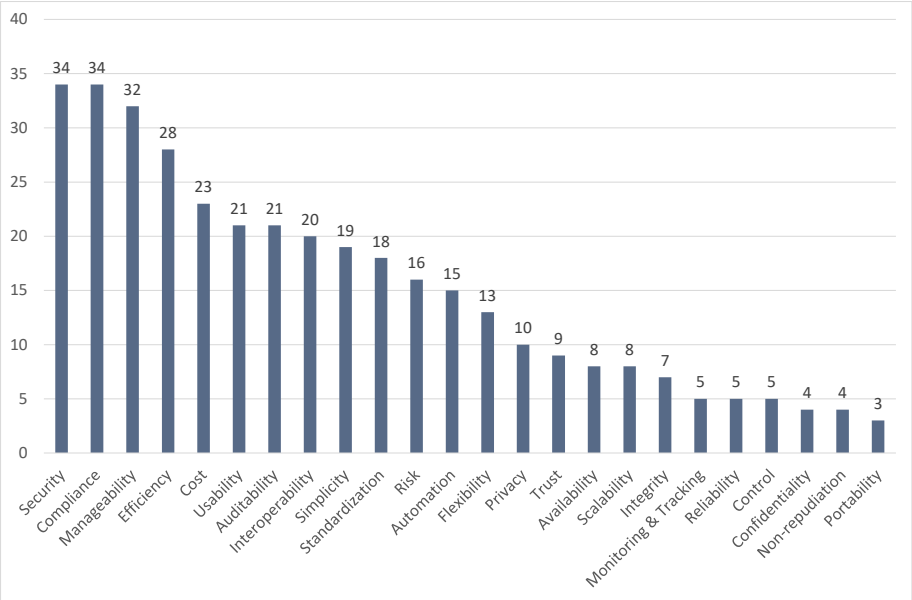
Table 1: Relevant literature identified in the systematic literature review (sorted by year).

#	Title	Author(s)	Year
1	"Privileged access management"	Haber	2020
2	"An overview of limitations and approaches in identity management"	Pöhn, Hommel	2020
3	"Contributing to current challenges in identity and access management with visual analytics"	Puchta et al.	2019
4	"The design of an identity and access management assurance dashboard model"	Damon, Coetzee	2018
5	"Measuring identity and access management performance – an expert survey on possible performance indicators"	Hummer et al.	2018
6	"Adaptive identity and access management — contextual data based policies"	Hummer et al.	2016
7	"Secure and usable enterprise authentication: lessons from the field"	Theofanos et al.	2016
8	"Advanced identity and access policy management using contextual data"	Hummer et al.	2015
9	"Role based access control architectural design issues in large organizations"	Asaf et al.	2014
10	"Centralized end-to-end identity and access management and ERP systems: a multi-case analysis using the technology organization environment framework"	Bradford et al.	2014
11	*Identity and access management: business performance through connected intelligence*	Osmanoglu	2014
12	"Privacy protection data access control"	M-Y Chen et al.	2013
13	"Towards a generic identity and access assurance model by component analysis – a conceptual review"	Damon, Coetzee	2013
14	"Qualitätssicherung im Identity-und Access Management"	Fuchs, Pernul	2013
15	"EIdM: concepts, technologies, and application fields"	Royer	2013
16	"From the IT authorisation to the role- and identity management"	Keszthelyi, Michelberger	2012
17	"Incorporating business strategy formulation with identity management strategy formulation"	Kruger, Mama	2012
18	*Identity management: concepts, technologies, and systems*	Bertino, Takahashi	2011
19	"Privacy-enhancing identity management in business"	Fairchild, Ribbers	2011
20	"The identity management challenge"	HA Smith, McKeen	2011
21	"The adoption of single sign-on and multifactor authentication in organisations: a critical evaluation using TOE framework"	D'Costa-Alphonso, Lane	2010
22	"Managing information access in data-rich enterprises with escalation and incentives"	Zhao, Johnson	2010
23	"Flexible authorisation in dynamic e-business environments using an organisation structure-based access control model"	T-Y Chen et al.	2009
24	"Enterprise identity management – towards a decision support framework based on the balanced scorecard approach"	Royer, Meints	2009
25	"Comparing identity management frameworks in a business context"	Hoepman et al.	2008
26	"Assessing the value of enterprise identity management (EIdM) – Towards a generic evaluation approach"	Royer	2008
27	"Enterprise identity management: what's in it for organisations?"	Royer	2008
28	"Preventative directions For insider threat mitigation via access control"	Sinclair, SW Smith	2008
29	"The challenge of federated identity management"	D Smith	2008
30	"Supporting compliant and secure user handling – A structured approach for in-house identity management"	Fuchs, Pernul	2007
31	"Access control for the services oriented architecture"	Li, Karp	2007
32	"Privacy policy enforcement in enterprises with identity management solutions"	Casassa Mont, Thyne	2006

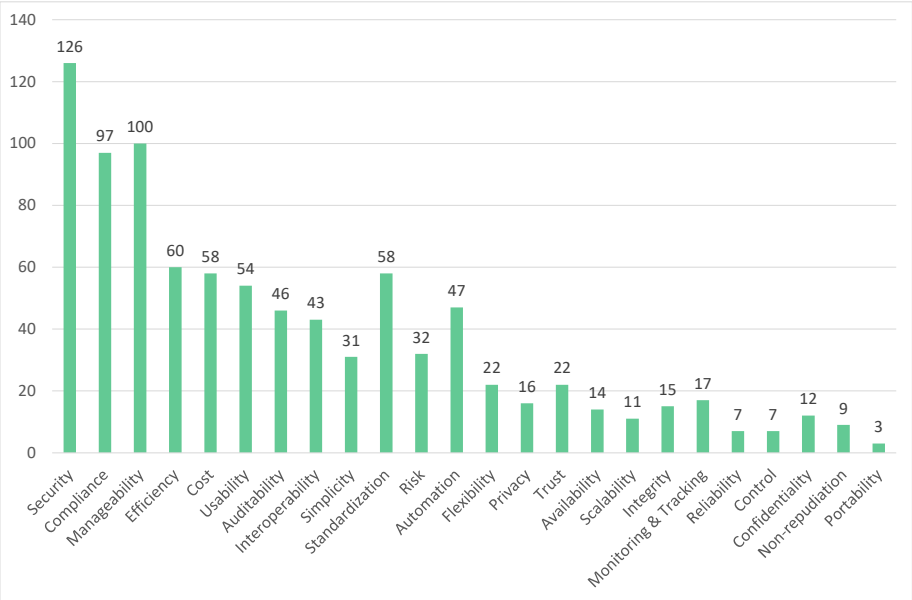
Table 1 continued on next page

#	Title	Author(s)	Year
33	"Identity and Access Control – demonstrating Compliance"	Sel, Van Rompay	2006
34	"Unify and simplify: Re-thinking identity management"	Small	2006
35	"Rule support for role-based access control"	Kern, Walhorn	2005
36	*Digital Identity: unmasking identity management architecture (IMA)*	Windley	2005
37	"Security and trust issues in ubiquitous environments – the business-to-employee dimension"	Walter et al.	2004
38	"Identity management"	Buell, Sandhu	2003
39	*On adaptive identity management: the next generation of identity management technologies*	Casassa Mont et al.	2003
40	"Task-role-based access control model"	Oh, Park	2003

A.2 Absolute Frequencies of the Codes After the First Cycle.



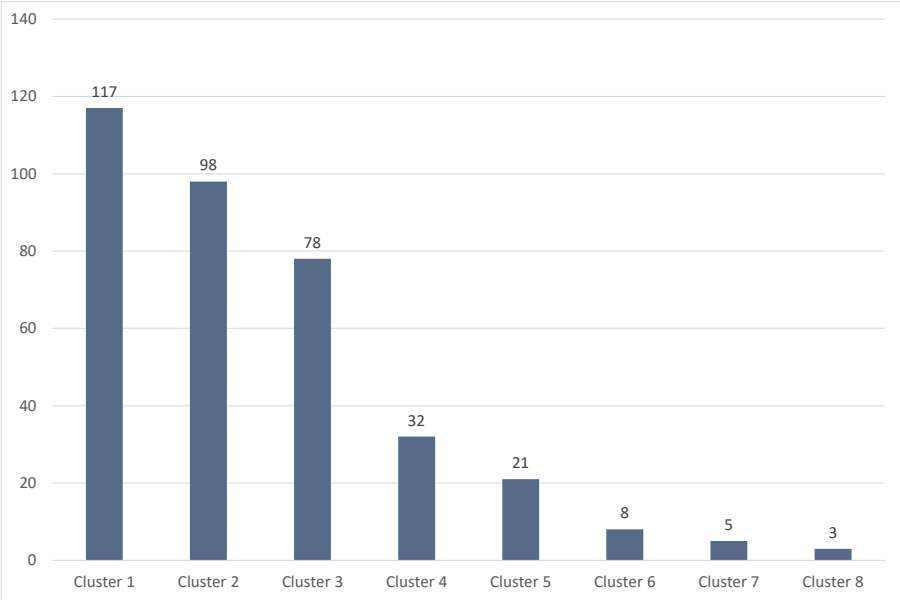
(a) Number of documents in which the codes occur.



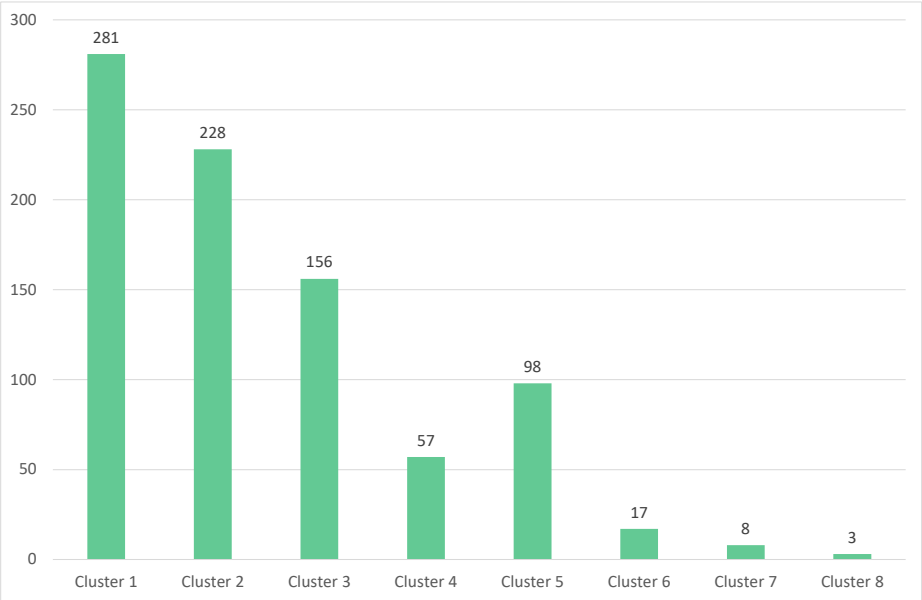
(b) Total frequencies of the codes.

Figure 1: Frequencies of all codes after the first cycle.

A.3 Absolute Frequencies of the Clusters



(a) Sum per cluster of the documents in which the mentioned codes occur.



(b) Total frequencies of the codes in each cluster.

Figure 2: Frequencies of all clusters.

A.4 Relations Between the Codes

Figure 3: Codes divided into clusters based on a distance matrix.

Table 2: Relations between the codes I.

	Security	**Compliance & Integrity**	**Manageability**	**Simplicity**	**Auditability**
Security	0	18	4	11	5
Compliance & Integrity	18	0	4	5	22
Manageability	4	4	0	3	2
Simplicity	11	4	3	0	1
Auditability	5	22	2	1	0
Efficiency	11	2	9	6	3
Cost	9	1	8	4	1
Standardization	5	6	2	12	1
Automation	0	8	10	2	5
Interoperability	3	1	2	5	0
Trust	3	6	1	0	2
Flexibility	0	0	0	1	0
Privacy	5	6	0	0	1
Availability	5	0	2	2	1
Portability	0	0	0	0	0

Table 3: Relations between the codes II.

	Efficiency	**Cost**	**Standardiz.**	**Automation**	**Interoperability**
Security	11	9	5	0	3
Compliance & Integrity	2	1	6	8	1
Manageability	9	8	2	10	2
Simplicity	6	4	12	2	5
Auditability	3	1	1	5	0
Efficiency	0	6	2	5	0
Cost	6	0	0	0	0
Standardization	2	0	0	2	12
Automation	5	0	2	0	0
Interoperability	0	0	12	0	0
Trust	0	2	1	1	1
Flexibility	0	1	0	0	0
Privacy	0	0	0	0	1
Availability	3	0	1	1	0
Portability	0	0	0	0	0

Table 4: Relations between the codes III.

	Trust	**Flexibility**	**Privacy**	**Availability**	**Portability**
Security	3	0	5	5	0
Compliance & Integrity	6	0	6	0	0
Manageability	1	0	0	2	0
Simplicity	0	1	0	2	0
Auditability	2	0	1	1	0
Efficiency	0	0	0	3	0
Cost	2	1	0	0	0
Standardization	1	0	0	1	0
Automation	1	0	0	1	0
Interoperability	1	0	1	0	0
Trust	0	1	9	0	0
Flexibility	1	0	0	0	0
Privacy	9	0	0	0	0
Availability	0	0	0	0	0
Portability	0	0	0	1	0

B Refinement and Interview-based Evaluation

B.1 Overview of Interview Partners

Table 5: Description of the interviewed experts.

#	Expert(s)	Field of Expertise	Experience
1	Expert 1: *(anonymized)*	IT Security and IAM	> 10 years
2	Expert 2: *(anonymized)*	Blockchain and IAM	> 4 years
3	Expert 3: *(anonymized)*	IT Management	> 10 years
4	Expert 4: *(anonymized)* Expert 5: *(anonymized)*	IT Management E-Commerce	> 5 years > 1.5 years
5	Expert 6: *(anonymized)* Expert 7: *(anonymized)*	SSI and Web Development SSI and Software Development	> 10 years > 10 years
6	Expert 8: *(anonymized)*	IAM	> 10 years; researcher in the field of IAM
7	Expert 9: *(anonymized)*	Blockchain and SSI	> 10 years
8	Expert 10: *(anonymized)*	SSI and IAM	> 10 years
9	Expert 11: *(anonymized)*	IT Management and E-Commerce	> 8 years
10	Expert 12: *(anonymized)*	IT Management and SSI	> 3 years

B.2 Interview Protocol

Table 6: Interview guideline.

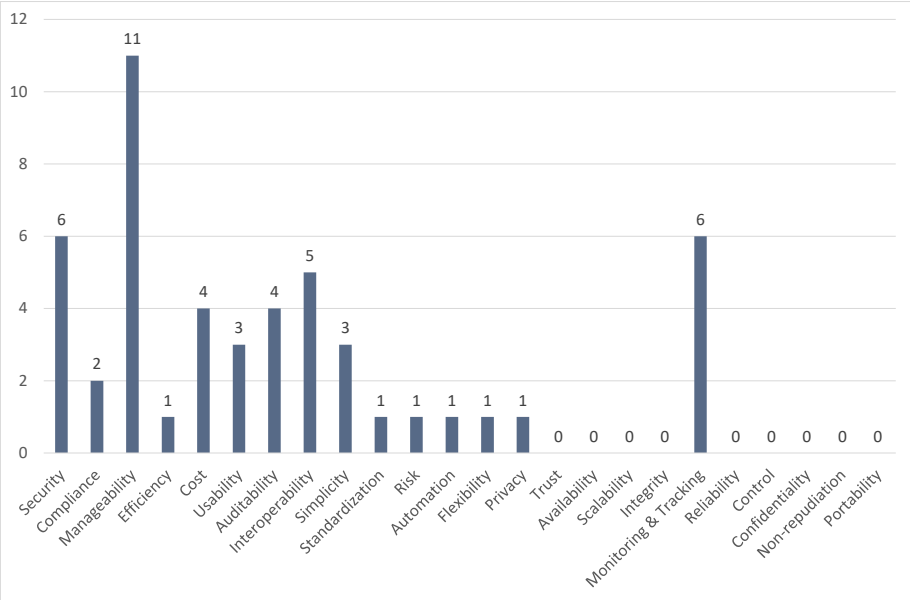
#	Parts and Questions
	Introduction
1	Greeting Obtain consent for recording and ask whether anonymization is desired How did you get in touch with IAM/SSI and what experience have you been able to make in this area?
	Current state of IAM
2	What benefits do you see for an organization by implementing an IAM system?
3	What are the possible drawbacks?
4	In which areas do you think there is still the greatest need to catch up?
5	What changes do you see as necessary?
6	Are there still aspects that need to be added?
7	Are there any points that should not be included?
	Presentation and evaluation of the prototype
8	Did you have any previous exposure to SSI? Brief explanation of SSI, if needed Presentation of the prototype
9	Do you have any questions regarding the prototype?
10	Which weaknesses do you see regarding the prototype? Which advantages do you think it may have?
	Feasibility of SSI in the field of IAM
11	Where do you see weaknesses or problems of an SSI-based solution?
12	Where do you see the advantages of an SSI solution compared to conventional approaches?
13	In which areas do you see the greatest benefits for SSI?
14	What do you currently see as SSI's biggest hurdles regarding adoption?
15	Do you think it is conceivable to introduce an SSI solution in companies?
16	Who do you consider to be responsible for issuing VCs in a company?
17	Do you think it makes sense to offer something like this internally to employees first?
18	Do you think it makes sense to offer something like this first as a possible alternative to traditional methods?
	Closing part
19	Do you have any final questions or suggestions you would like to add? Farewell

B.3 Codebook Excerpt

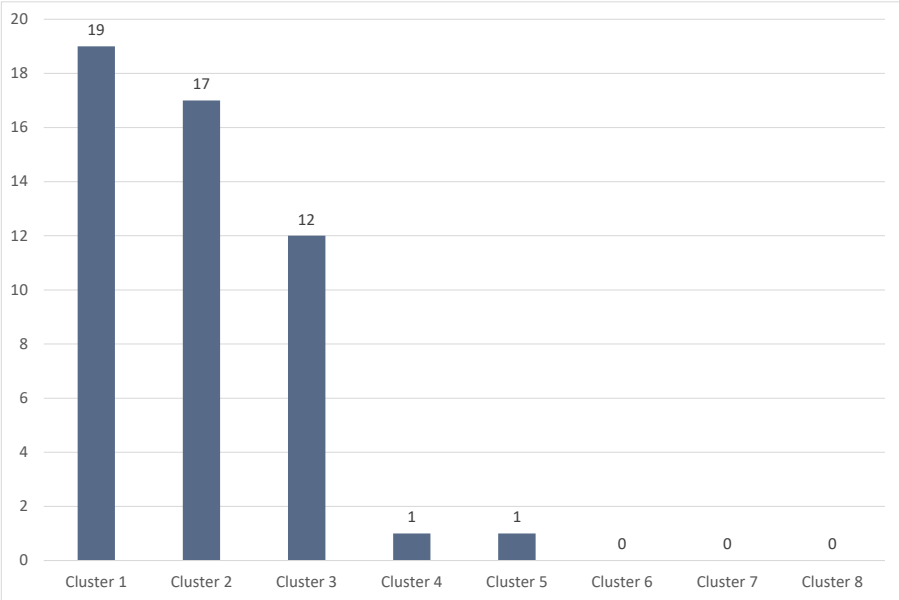
Table 7: Example codes.

Code	Subcode	Example Quote
User	Usability	So that means we have an incredible opportunity to cut stuff out of this identity and access lifecycle or dramatically improve the complexity and usability of it. (Expert 10)
	Privacy	I think the advantages for users are obvious: privacy, etc. (Expert 2).
	Control	Concepts like giving the user or the citizen control over their stuff, that requires quite a change in mentality. (Expert 11)
	Transparency	What I think is an advantage, or what I can think is an advantage, is that I actually have, let me say, full transparency in this wallet at all times. (Expert 1)
	Portability	Because you mentioned operability and portability: If you're using the esatus wallet now and then you say, hey I think the Trinsic is actually much more awesome, I want to switch over it, can that be done? (Expert 6)
Enterprise	Automation	Then you will be automatically redirected back to the login and will not be able to access it again. (Expert 6)
	Security	Usability and security, that's what SSI focuses on to a certain extent and also combines both. (Expert 7)
	Fast onboarding	Just flexibility in onboarding, you get your people, new employees integrated into the systems much faster. (Expert 7)
	Only one system	Even though they might be ten times as big, but then I only have one and I can just accommodate those restrictions on who can share what where in that one system. (Expert 2)
	Simplicity	So simplification is actually my main point. (Expert 4)

B.4 Absolute Frequencies of the Clusters



(a) Number of interviews in which the codes occurred.



(b) Sum of the mentioned codes per cluster.

Figure 4: Mentioned codes during the expert interviews.

B.5 Potential Improvements Through SSI-based IAM

Table 8: Sample quotes from the experts on improvements in each of the four IAM requirement clusters.

Cluster	Requirement	Example Quote
Security & Compliance	Auditability	I know exactly who has logged into my systems, where, and when. I can trace that back. (Expert 9)
	Security	And then if they [A/N: employees] resign or leave or are fired, then blocking them in the systems [...] is also faster. I think the technology stack [A/N: SSI], even if it still has weaknesses [...] is strong. With the revocation of keys, the technology stack generally resolves this tension between usability and security quite well. (Expert 7)
Operability	Automation	But for that, that is, for pure onboarding, [. . .] that could definitely be automated [A/N: with SSI]. (Expert 8)
	Efficiency	On the one hand, you can integrate your new employees into the systems much faster, or rather you grant them access to the systems more quickly. And then when they resign or leave or are laid off, they're also locked out of the systems faster. (Expert 7)
	Manageability	We have a very simplified onboarding process and, of course, a maximally simplified offboarding process for the leaver case, [...] I press revoke, the authorization is revoked, which means [users] can no longer prove that [they] can get in somewhere, and that's it. (Expert 10)
User	Control	What I think is an advantage [...] is that I actually have full transparency in this wallet at all times [...] about who has somehow already queried my credentials then perhaps could also somehow consolidate the whole thing at once and in principle say [...] I somehow don't want to use them anymore [...]. (Expert 1)
	Control & Privacy	That now very specific data is transferred [...] has a lot of advantages regarding data minimization from my perspective, because users submit their data consciously. (Expert 7)
	Privacy	Privacy by design, yes. The fact that the [A/N: SSI] test stack itself, the way it's designed, provides, yes, very simple data sovereignty that you didn't have before with any other technology. (Expert 7)
	Simplicity	The fact that you don't have to come up with a different password for each system, or any password at all, but have the password in your wallet that you need to unlock your smartphone, or the biometric feature, makes it convenient. [...] There is a terminal where you then just have to show your cell phone and [...] then the entire thing would be processed. [...] That would make such a thing [A/N: SSI-based solution] very convenient. (Expert 3)
Technology	Interoperability	I think if you want to demonstrate the power of SSI, then you should practically show how independent this credential is from this one company, that you don't have to use it only with the company that issued it. And [...] show that credentials are much more powerful than a simple OAuth. (Expert 6)
	Portability	It's very nice that this is a standard that has been approved by the W3C. Which [...] at least in the future can be integrated by many different systems and accordingly then also the portability increases and you can use your identity maybe across different networks if the networks trust each other. (Expert 6)

C Prototype

C.1 Form to Issue a Credential

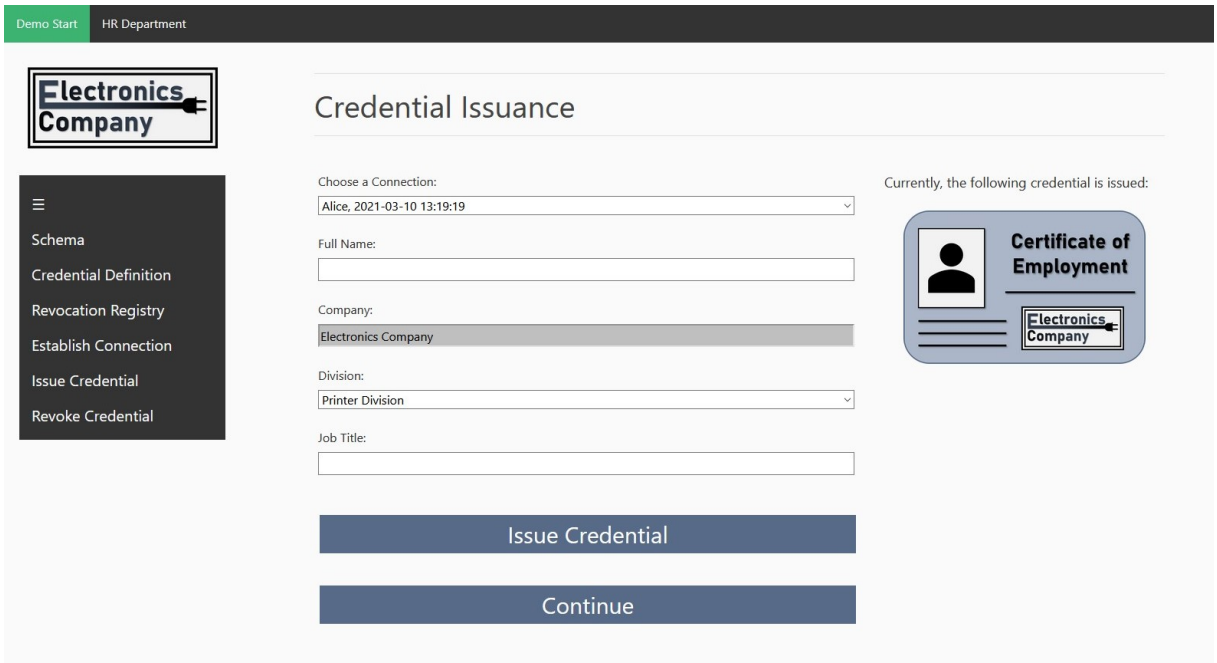
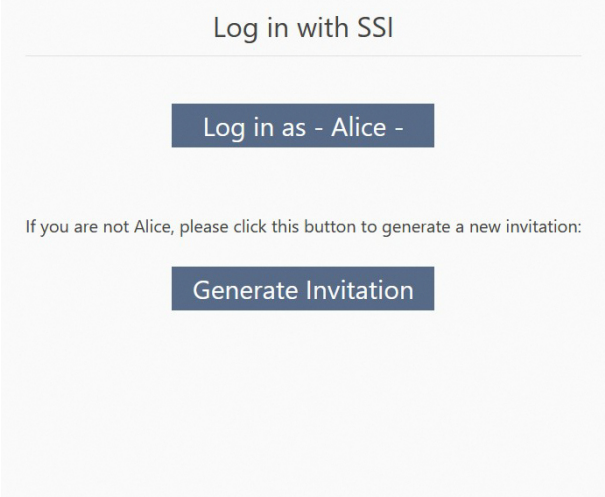


Figure 5: Form to issue a credential.

C.2 View of the "Login" Page

(a) View for new user.



(b) View for returning user.

Figure 6: View of the "login" page for new and returning users.

C.3 Proof Request

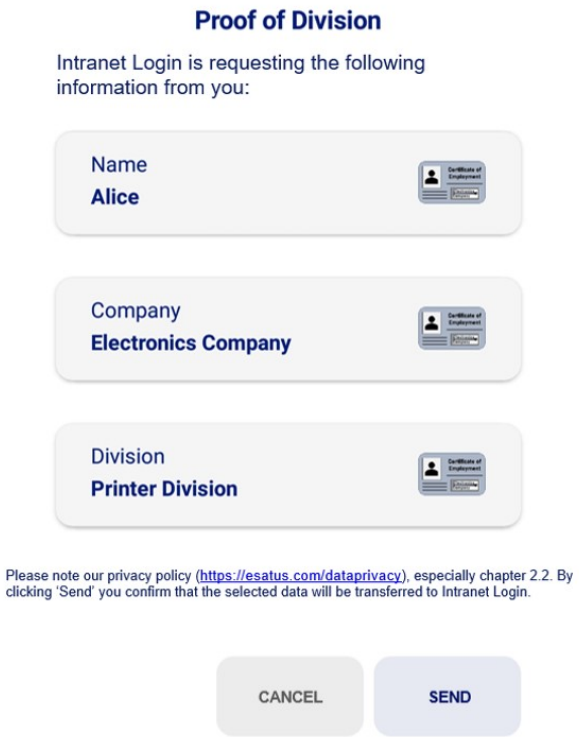


Figure 7: Answering the proof request with the wallet app.

C.4 Verifiable Presentation

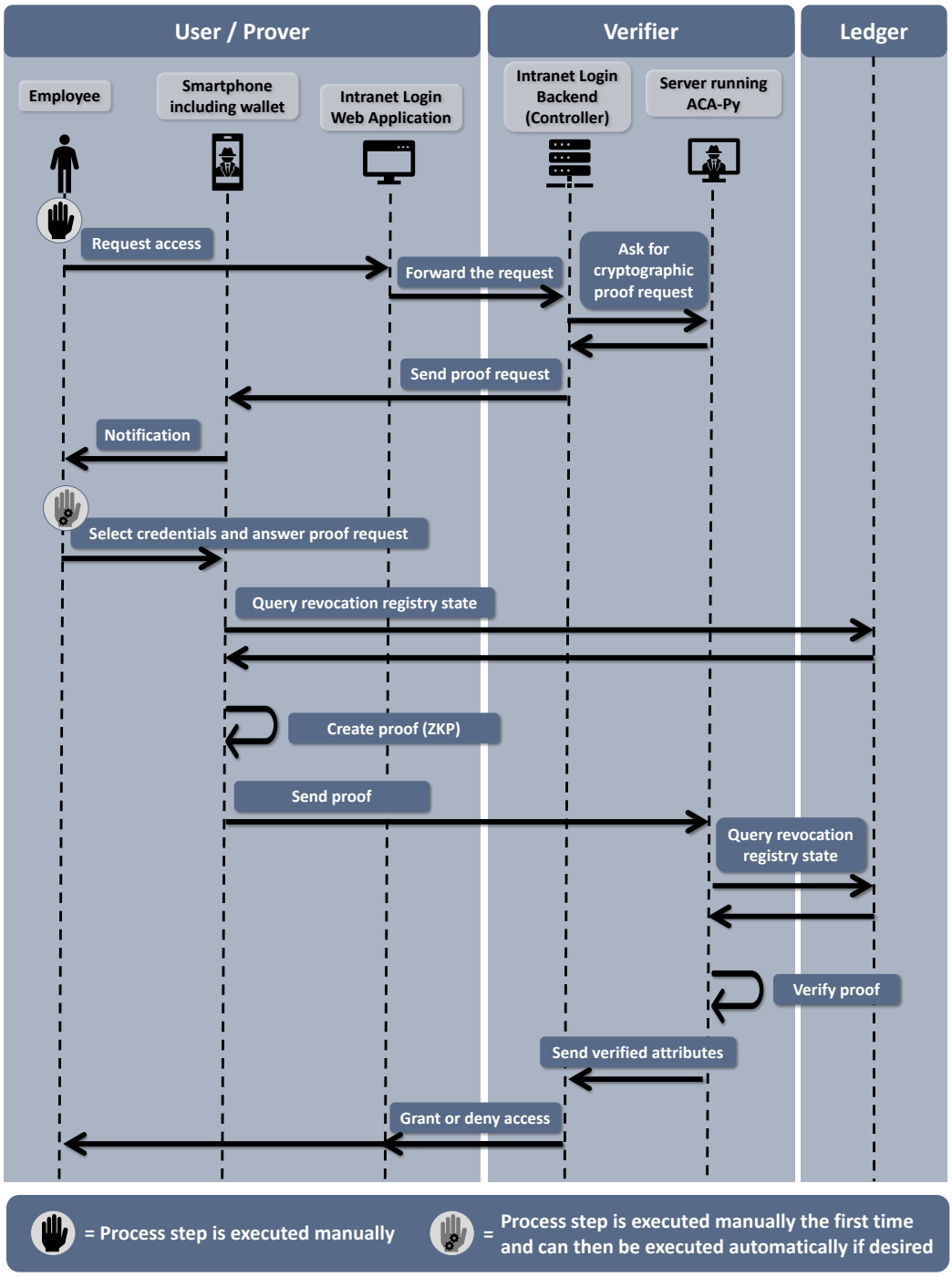


Figure 8: Sequence diagram for the verifiable presentation.