H. Roßnagel, C.H. Schunck, J. Günther (Hrsg.): Open Identity Summit 2023,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 27

Lifting the Veil of Credential Usage in Organizations: A Taxonomy

Ricardo Bochnia, Daniel Richter, Jürgen Anke[1]

Abstract: With the emergence of self-sovereign identity (SSI) as a paradigm for digital identity management the handling of verifiable credentials (VCs) has become an important topic in organizations. Organizations process a wide variety of documents which can be considered credentials. Previous research shows that a challenge in developing SSI systems is a lack of understanding of the core aspects of the paradigm and their relation to existing organizational practices. Our research focuses on the different characteristics of credentials in organizations and maps the characteristics of VCs to physical credentials. Our findings indicate that credentials in organizations can be classified by ten dimensions. Additionally, VCs have many possible characteristics of physical credentials, although implementation and support for certain features may be vendor-specific. Finally, we provide insights and suggestions for SSI researchers and developers.

Keywords: Taxonomy; Organizational Credential Management; SSI; Digital Identity

1 Introduction

Self-sovereign identity (SSI) is an emerging paradigm for digital identity management, attracting interest from scholars, identity experts, public institutions, and private enterprises alike [Se22]. While SSI rests on a set of principles with the primary goal of empowering private persons to control the usage of their data [SC22], the implementation of the paradigm offers a set of benefits exceeding better data protection. Among them are potentials especially for organizations to provide services with a higher degree of automation, a streamlined service experience as well as higher data quality [JRA22; LKA21; RA21]. These potentials are linked to the technical foundations SSI is building on. At its core lies the exchange of verifiable credentials (VCs), which can be stored in wallet applications [Eh21]. VCs are tamper-resistant data containers, which allow to prove the origin of the data as well the authorization to use them [SLC22]. The VC data model offers the flexibility to digitize almost any physical document used in proof processes undertaken by private persons and organizations as well as between either of those [Se21].

To reap the above-mentioned benefits of SSI it is necessary to provide a functional technical infrastructure supporting the exchange of VCs [LKA21]. While some research has been

[1] HTW Dresden, Digital Service Systems Group, Friedrich-List-Platz 1, 01069 Dresden, Germany
{ricardo.bochnia, daniel.richter, juergen.anke}@htw-dresden.de

doi:10.18420/OID2023_02

carried out on the properties of mobile wallet applications for private persons [PAZ22; Sa22], we focus in this research paper on the role of organizations in the SSI paradigm. Previous research shows that a fundamental challenge in developing SSI systems is a lack of understanding of the core aspects of the paradigm and how they relate to existing organizational practices [LKA21; Se21]. Since organizations process a wide variety of documents which can be considered credentials it can be hard to relate this complexity to requirements for the components of SSI systems such as VCs and digital agents. As a first step we therefore wish to provide a better understanding of the properties of credentials used in organizational practice by answering the research questions: *"What types of credentials do organizations interact with?"* and *"How do VCs map to the characteristics of physical credentials?"*

Methodologically, we conducted a multi-case study of credentials employed by organizations in the ID-Ideal consortium[2], which researches digital identities in business and administration, to construct an initial taxonomy highlighting characteristics relevant to SSI system development. The intended use of the taxonomy lies in aiding practitioners to identify candidates for the creation of VCs in business processes and to map their properties to SSI system requirements. Furthermore, we would like to highlight gaps between physical and verifiable credentials, which need to be closed by SSI developers.

The remainder of the paper is organized as follows: The background section provides a brief introduction on credentials. The method section details the taxonomy building process and data sources. The main part of the paper presents the proposed taxonomy along the identified dimensions and corresponding characteristics for credentials in organizations. The discussion section provides a critical analysis of the results and their implications for the management of credentials in organizations as well as recommendations for future research. Finally, the conclusion summarizes the main findings.

2 Background

In its most common sense, the term credentials refers to those documents proving a person's identity or qualifications [SLL20]. In identity management the concept of credentials is broader in its scope, focusing more on structure than content. VCs therefore are defined as a set of claims made by an issuer about a specific subject [SLC22]. By referencing the issuer and providing security mechanisms such as digital signatures, a credential can be used by its holder to prove the attributes of the subject to a verifier trusting that issuer.

Organizations often act as issuers and verifiers of credentials for individuals, e.g. identity documents, customer cards, transport tickets. However, credentials are also used in transactions between organizations [PR21]. Examples are commercial register excerpts, ISO certifications, as well as different types of bills. Organizations use a wide variety of

[2] https://id-ideal.de/en/

credentials with different properties along the full spectrum of possible operations, and with a high frequency. Additionally, organizational structure requires granting different levels of access to credentials [PR21]. Compared to wallet applications for private persons, the credential usage of organizations leads to a set of more comprehensive requirements for SSI agent software for organizations [PR21]. Current SSI agent solutions often provide only basic functionality, such as issuance and verification, lacking advanced features for credential handling [OR21]. This may be due to a focus on technical purity and premature interoperability over practical business functionality [OD22; OR21].

3 Method

We developed our taxonomy using the Extended Taxonomy Design Process (ETDP) and its corresponding Taxonomy Design Recommendations (TDR) by Kundisch et al. [Ku22] as shown in Figure 1. The ETDP is an extension of the methodology of Nickerson et al. [NVM13] and applies Design Science Research (DSR) to treat the taxonomy as an artifact that needs to be evaluated for its usefulness [Ku22]. The data for this study was collected from a multi-case study of use cases from the ID-Ideal consortium, which covers a diverse range of real-world scenarios such as authorities, public transport, car sharing, industry 4.0, education as well as a review of relevant literature. This data was analyzed to identify common characteristics of credentials in organizations.

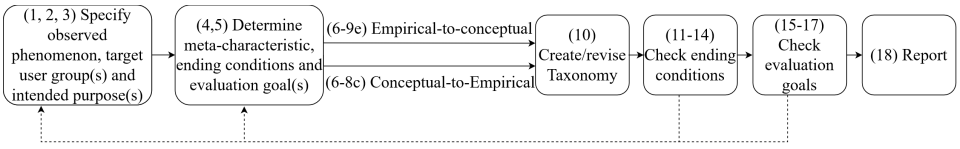

Fig. 1: Abbreviated representation of EDTP based on [Ku22]

The ETDP is an iterative approach and consists of eighteen steps. The first three steps define the observed phenomenon, the target user group, and the intended purpose of the taxonomy. The fourth step determines the meta-characteristic that defines what is and is not relevant for the taxonomy design. In the fifth step, the ending conditions for the taxonomy design and the evaluation goals are defined. Steps six through ten offer two approaches for building the taxonomy: empirical-to-conceptual and conceptual-to-empirical. In the empirical-to-conceptual approach, objects are considered first and dimensions are derived from them. In the conceptual-to-empirical approach, dimensions are conceptualized first and then objects are placed into them. After the taxonomy has been created, the objective and subjective ending conditions are checked in steps eleven to fourteen. If these conditions are met, steps fifteen through seventeen evaluate if the evaluation goals were achieved. The last step is reporting the taxonomy after successful evaluation.

The observed phenomenon for our research was the interaction with credentials in organizations. Our target group for this taxonomy is researchers and developers of SSI solutions,

particularly those who work with wallets and agents. The purpose of this taxonomy is to serve as a foundation for developing SSI solutions for organizations. Our meta-characteristic underwent revision throughout our process, initially starting as "How is the credential handled?" but eventually evolving into "handling of credentials in organizations in the perspectives of representation, content and processing". We adopted the objective and subjective ending conditions from Nickerson et al. [NVM13]. For our taxonomy building, we primarily followed the empirical-to-contextual approach, as our focus was to capture the current status in handling credentials. But we also did a contextual-to-empirical iteration to extend our taxonomy as recommended by TDR. For our evaluation we selected new objects and characterized them using our taxonomy. We included at least some objects from domains not considered during the design of the evaluation to find gaps in our taxonomy. These evaluations helped us to revise our dimensions and characteristics.

4 A taxonomy of credentials in organizations

The resulting taxonomy is displayed in Figure 2. It consists of ten dimensions which can be organized into the three perspectives representation, content and processing which are elaborated in the following sections. An exemplary classification of a credential can be found in Figure 3.

	Dimension	**Characteristics**					**E/N**[1]
Representation	*Holder Type*	Natural Person	Legal Person	Thing			E
	Transferability	Transferable	Non-transferable				E
	Representative	Bearer	Guardian	Delegate	Controller	None	E
Content	*Validity*	Number of uses	Time	Revocation	Unlimited		N
	Modifiability	Modifiable	Non-modifiable				E
	PII	Sensitive	Normal	None			E
	Data Type	Text	Image	Other			N
Processing	*Data Retention*	Original	Copy	Transcript	None		N
	Automation	Fully	Partial	Manual			E
	Trustworthiness	High	Medium	Low	None		E

[1] Exclusivity of characteristics for a given dimension. E = Mutually exclusive characteristics. N = Non-exclusive characteristics.

Fig. 2: A taxonomy of credentials in organizations

4.1 Representation

Natural persons have the capability to make decisions and act independently in many situations. However, *representation* is still important for them in certain circumstances, such as when they are unable to act on their own or when they need to delegate authority. In organizations, representation is of even greater significance as they can not act independently but need to be represented by their organs. Three dimension have been identified that help to understand representation: Holder Type, Transfer and Representative.

Holder Type. The holder of a credential can be a natural person, legal person, or a thing. In a general sense, individuals and legal entities are often the holders of credentials, although things can also be holders. For example, product certificates can be viewed as being held by the corresponding product, such as the QR code on AMD's Ryzen CPU box, which verifies the authenticity of the corresponding CPU.

Transferability. If a credential is transferable, it means that its holder has the ability to pass it on to another party, which becomes the new holder. The conditions under which it can be transferred must be specified. Non-transferable credentials include ID cards or trade licenses.

Representative. This dimension describes the relationship between the subject of a credential and its holder. In the case of bearer credentials possession alone is sufficient for using the credential [SLL20]. Thus, there is no subject to represent. An example would be single ticket for public transport. When the holder and subject are the same, then there is no representation and it is an identifying credential. True representation only exists in three cases: guardian, delegate, and controller. A guardian is a person who has been appointed by a legal authority to make decisions on behalf of someone who is unable to make decisions for themselves, such as a minor child. A delegate is given the authority and responsibility to perform limited tasks on behalf of another, such as a CEO representing a company. Generally, a delegate possesses greater autonomy and discretion in carrying out their assigned tasks than a guardian, who is subject to more direct oversight and must act in accordance with the wishes of the entity they are representing. A controller controls a thing that is inherently incapable of acting autonomously, e. g. a drone that needs to be manually operated [SO19].

4.2 Content

This perspective focuses on the *content* of the credential. It features the following dimensions: Validity, Modifiability, Personally Identifiable Information (PII), Data Type and Trustworthiness.

Validity. Credentials vary in terms of their validity. Some credentials can only be used once, such as a concert ticket, or a fixed number of times, such as a four-trip public transport ticket. Different time limits are also possible, for example, a ticket may be valid one

year after issuance. A combination of number of usage and time constraints is common. Additionally, credentials can be revoked due to numerous reasons such as the violation of traffic regulations in the case of a driving license. In contrast, some credentials, such as a birth certificates, are considered to be valid unlimitedly if they are free of factual errors.

Modifiability. Some credentials can be modified lawfully, while others can not. For instance, the address of a German ID card be updated by an official address sticker. However, if a surname change occurs after marriage the ID card can not be updated and is considered invalid. Instead, a new ID card is issued which is not a modification. The difference is due to the fact that an ID card is valid for six or ten years (depending on the holder's age) and address changes occur much more frequently during this period. Not every claim has to be modifiable, usually only claims that may change frequently are modifiable. Modification usually makes sense if the effort is less than for a re-issue. Sometimes modification is part of creating a credential as for the pilgrim's credential of the Way of Saint James [SLL20].

PII. PII refers to any information that can be used to identify an individual. It is a major concern for organizations that handle credentials due to data protection regulations such as the General Data Protection Regulation (GDPR). If a credential contains normal or even sensitive PII the credential handling must comply with these regulations. Which PII is considered sensitive is regulated differently in each jurisdiction. However, certain categories such as biometric data are often considered sensitive across jurisdictions.

Data Type. Although credentials with only text or text and image data are common, there are credentials which only contain image data, e. g. stamps used during festivals or a badge with only the photograph of the holder and the logo of the issuing institution [SLL20]. Other data formats are also possible. For instance, smart cards can contain data besides text and image such as biometric data.

4.3 Processing

While the *processing* of credentials is also done by individuals, the scale is much greater for organizations. This perspective consists of the following dimensions: Data Retention and Automation.

Data Retention. Data retention refers to how the data is retained during the handling of a credential. There may be no retention at all. Invoices usually have to be archived by law and are therefore kept as an original. During Videoident, a video identification process, an image of the ID card's front and back side is captured which is a copy of the credential in the form of an image. Copies are often in a different format than the original credential and may be an accepted substitute for the original credential. If only the ID card number is written down during the process, it is a transcription of the credential which contains just certain claims of the credential. Transcriptions can not be used as substitute for a credential but may be used for non-repudiation. Issuers usually transcribe at least part of the processed

credential data. The same may apply to verifiers. A combination of different data retention approaches such as copy and transcript is possible.

Automation. The processing of a credential can be automated to certain degrees. At the moment credential issuance and verification often involves manual labor and is at best partially automated which is more time consuming than automated processing. Few credentials, such as VCs, offer the possibility for fully automated credential processing.

Trustworthiness. Finally, credentials can be differentiated by their trustworthiness. For digital credentials the level of assurance, which are defined in frameworks such as eIDAS, NIST SP 800-63, or ISO 29115, can be a guideline to determine how trustworthy a processed credential is. However, there are no universal standards or norms that explicitly address physical credentials, as the requirements and context for physical credentials are often industry or country specific. The required trustworthiness depends on the use-case. Lower trustworthiness might be acceptable for a better user experience or lower costs if potential damage is minimal. Untrustworthy credentials include detected forged ones.

4.4 Example Classification

	Dimension	Characteristics				
Representation	*Holder Type*	Natural Person	Legal Person	Thing		
	Transferability	Transferable	Non-transferable			
	Representative	Bearer	Guardian	Delegate	Controller	None
Content	*Validity*	Number of uses	Time	Revocation	Unlimited	
	Modifiability	Modifiable	Non-modifiable			
	PII	Sensitive	Normal	None		
	Data Type	Text	Image	Other		
Processing	*Data Retention*	Original	Copy	Transcript	None	
	Automation	Fully	Partial	Manual		
	Trustworthiness	High	Medium	Low	None	

Fig. 3: Example: public transport subscription ticket which is checked by an inspector.

To clarify the taxonomy, we provide an example classification of a public transport subscription ticket which is checked by an inspector in Figure 3. The ticket is held by a natural person but can be transferred to another person. It is a bearer credential since the credential can be used by anyone who possesses it. The subscription is valid until revoked, but the smart card that contains the ticket is only valid for up to five years and must be replaced for an update. The card is non-modifiable, identified only by a card number, and thus contains no PII. It is an credential with both text and image data. The inspector scans the ticket using a validation device in a partially automated process, which does not retain any data throughout the procedure. The trustworthiness is only medium since, although

the inspector trusts the issuers issuance process, there is no way to ensure the credential's possessor is legitimized by owner.

4.5 Comparing physical and verifiable credentials

To replace existing physical credentials, VCs should possess many of the possible characteristics of physical credentials. But as business processes can be redesigned with VCs, exact replication isn't necessary. Below, each perspective will be examined individually. Key differences are outlined in Table 1.

Perspective	**Dimension**	**Difference**
Representation	Transferability	Support is vendor-specific
	Representative	Support is vendor-specific
Content	Validity	Number of uses constraint unsupported
	Modifiability	No modification besides refresh possible
Processing	Data Retention	Retention of original not advised
	Automation	Optimized for automated processing

Tab. 1: Key differences between verifiable and physical credentials according to our taxonomy

The specification states that "Verifiable credentials are not an authorization framework and therefore delegation is outside the scope of this specification. However, it is understood that verifiable credentials are likely to be used to build authorization and delegation systems" [SLC22]. Thus, representation may be feasible with VCs but support is vendor-specific. This applies to the dimensions transfer and representative. Although the standard mentions these topics, they are currently non-normative. A VC can be held by a thing, a natural or legal person, hence all holder type characteristics are possible.

In terms of validity, VCs do not support a number of use constraint. Modification is not mentioned by the specification and thus not supported. Only a refresh service for expired credentials exists. All characteristics of the other three dimensions PII, Trustworthiness and Data Type are supported by VCs.

In terms of data retention, all characteristics are possible, but retaining the original is not recommended since data minimization is preferred. VCs support both fully and partially automated processing, as well as manual processing. Although, manual processing is limited by the fact that a human cannot verify the signature without supporting technology.

5 Discussion

We have identified ten dimensions of credentials used by organizations that are relevant for SSI development as presented in Figure 2. Further, we identified six of these ten dimensions

in which VCs differ from physical credentials as shown in Table 1. Implications for agent and wallet development are given in Table 2 and selected examples are explained in more detail down below.

5.1 Implications

The perspective representation is particularly relevant in the development of agents and wallets for organizations. It involves considering the various types of holders that will be interacted with. Depending on the type of holder, the interaction may be via a graphical user interface (GUI) for natural persons, application programming interface (API) for things, or a combination of both for legal persons. Regarding Transferability and Representative of VCs more standardization is necessary.

Perspective	**Dimension**	**Relevance in Agent/Wallet Development**
Representation	Holder Type	Interaction via GUI, via API or a combination of both
	Transferability	How to transfer credentials to another wallet? How can the verifier see that the transfer is rightful?
	Representative	How are different cases of representing another entity managed?
Content	Validity	Possibility to renew the credential when presenting the old credential and possibly other credentials. In case of multi usage it must been tracked somewhere (e.g. by new updated credential) how often the credential was used.
	Modifiability	How is a credential modified? Does the credential contain a modification history?
	PII	Compliance with data protection regulations like the right to be forgotten
	Data Type	Image processing is more complex but offers opportunities.
	Trustworthiness	Trusted issuer/verifier/holder list, auto-proof/accept of credential
Processing	Data Retention	Non-repudiation, audit log
	Automation	Integration in automated workflows

Tab. 2: Perspectives and Dimensions and their relevance in Agent/Wallet Development

The handling of PII is another important consideration. It is crucial for agents and wallets to handle PII in a way that is compliant with data protection regulations. This includes the right to be forgotten, thus in blockchain-based solutions no PII should be stored on-chain. For a more detailed discussion regarding PII and SSI, see Kondova et al. [KE20].

Data type is another important dimension to consider. Currently many VCs are text-based but small images are rather common in physical credentials. Although image processing is generally more complicated than text processing, it offers some opportunities. One example is the use of facial recognition technology. By including a photograph of the credential holder in the VC, it is possible to use facial recognition to verify the identity of the holder

by matching their face to the one in the credential. This can be done in real-time through a live stream, and can be performed either by a human or through automated technology. This method can help prevent fraud and impersonation, especially in contexts where a high degree of trust is required, such as financial or healthcare settings.

The trustworthiness of credentials is a critical consideration as the problem of forged credentials is significant in certain areas such as using a fake ID to purchase alcohol [DS22]. With the emergence of VCs, it has become easier to determine the authenticity of a credential compared to many physical ones, which is prerequisite for trustworthiness. However, to determine the trustworthiness of a credential, agents and wallets must perform more than simply verifying the cryptographic proof. To ensure trustworthiness, agents and wallets may need to consult a trusted issuer list or display in the GUI that the presented credential is from a trusted issuer or verifier. With such trusted parties, credentials may be automatically accepted or presented without user intervention, streamlining the issuance and verification processes.

Regarding the number of usage constraints workarounds are possible, e.g. it is possible to represent a physical 10-ticket by 10 single VC tickets. But it should be done in user friendly way, e. g. grouping them in the wallet UI. This may be preferable to a complex solution that tries to track the number of uses constraint as part of the credential.

The developers of SSI must strive to enhance the modifiability capabilities of VCs. While revoking and issuing an updated credential may be suitable for certain use cases, it may not be feasible in situations where the modification is performed by a party other than the original issuer. This approach can also lead to confusion for users. For example, in the case of a public transport ticket that is validated using a ticket validator, revoking the original ticket and issuing a new one may be confusing, as it is more intuitive for the ticket to simply be modified to reflect its updated status like it is done with a physical ticket. Furthermore, revoking and reissuing a VC can impact trust in the VC, as it suggests that there was a problem with the original VC and raises questions about its reliability.

5.2 Limitations

The limitations of the study include being based on use cases from the ID-Ideal project which are mainly from the public sector. While the use cases from ID-Ideal and our literature review are diverse and offer valuable insights into how organizations handle credentials, they are not exhaustive. Therefore, it is possible that a more diverse sample of organizations from different industries would lead to an expansion of the taxonomy to include new dimensions or characteristics. We further note that trust between the holder, verifier and issuer is crucial. Although trustworthiness was included in the taxonomy as a single dimension, it is rather complex and consists of several factors such as issuance and verification process quality. How trustworthiness is exactly determined depends on the appropriate governance framework for the given credential. Since there are numerous governance frameworks for

credentials, our four levels of trustworthiness should be considered as a guide, and it may be appropriate to replace them in practice with the levels from the applied framework.

5.3 Further Research

In order to validate the proposed taxonomy and gain a more comprehensive understanding of the different types of credentials used by organizations, future work should include a larger sample of organizations from various industries and consider possible new dimensions or characteristics. Another option is to develop an industry-specific taxonomy by examining use cases within a single industry, which could then serve as the foundation for an industry-specific SSI solution.

The trust relationship between actors should also be studied in more depth, as it could impact the development of SSI solutions, such as auto-proof or auto-accept of trusted credentials. Additionally, SSI wallets and agents for organizations are required for credential management but are under-researched. It would be useful to look more closely at the requirements that organizations have for these systems.

6 Conclusion

In conclusion, this paper presents an initial credential taxonomy addressing the lack of credential classifications in organizations. Our findings indicate that organizations interact with various credentials classified by ten dimensions: holder type, transferability, representative, validity, modifiability, PII, data type, trustworthiness, data retention, automation.

Our research also shows that VCs already have many characteristics of physical credentials, although implementation and support for certain features vary by vendor. This highlights the importance of further standardization in the field, in order to ensure that VCs are handled and processed in a consistent and secure manner. Insights gained from our research will contribute to the development of effective and secure SSI solutions for credential management and provide a valuable framework for understanding the different dimensions of credentials in organizations, serving as a foundation for further research in the field.

References

[DS22] DSA: Counterfeiting of driver's licenses, 2022, `https://www.documentsecurityalliance.org/forms/Securing-Drivers-Licenses.pdf`.

[Eh21] Ehrlich, T. et al.: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD Praxis der Wirtschaftsinformatik/, PII: 711, 2021.

[JRA22] Jürgenssen, O. et al.: Selbstbestimmte digitale Identitäten in der Smart City, Potenziale und Grenzen. In. Gemeinschaften in Neuen Medien. TUDpress, Dresden, pp. 148–158, 2022.

[KE20] Kondova, G. et al.: Self-sovereign identity on public blockchains and the GDPR. In: The 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, March 30-April 3, 2020. Pp. 342–345, 2020.

[Ku22] Kundisch, D. et al.: An Update for Taxonomy Designers. Business & Information Systems Engineering 64/4, PII: 723, pp. 421–439, 2022.

[LKA21] Laatikainen, G. et al.: Self-Sovereign Identity Ecosystems: Benefits and Challenges. In: 12th Scandinavian Conference on Information Systems, Living in a digital world? IRIS, Orkanger, Norway, 2021.

[NVM13] Nickerson, R. C. et al.: A method for taxonomy development and its application in information systems. European Journal of Information Systems 22/3, 2013.

[OD22] O'Donnell, D.: Premature Standardization & Interoperability, 2022, https://www.continuumloop.com/premature-standardization-interoperability/.

[OR21] O'Donnell, D. et al.: Digital Wallet Report 2021 UPDATE, 2021, https://www.continuumloop.com/the-wallet-report-update/.

[PAZ22] Podgorelec, B. et al.: What is a (Digital) Identity Wallet? A Systematic Literature Review. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, pp. 809–818, 2022.

[PR21] Preukschat, A. et al.: Self sovereign identity. Manning Publications, 2021.

[RA21] Richter, D. et al.: Exploring Potential Impacts of Self-Sovereign Identity on Smart Service Systems. Business Information Systems/, pp. 105–116, 2021.

[Sa22] Sartor, S. et al.: Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. ECIS/, 2022.

[SC22] Schardong, F. et al.: Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors (Basel, Switzerland) 22/15, 2022.

[Se21] Sedlmeir, J. et al.: Digital Identities and Verifiable Credentials. Business & Information Systems Engineering 63/, PII: 722, pp. 603–613, 2021.

[Se22] Sedlmeir, J. et al.: Transition pathways towards design principles of self-sovereign identity. In: Proceedings of the 43rd International Conference on Information Systems. 2022.

[SLC22] Sporny, M. et al.: Verifiable Credentials Data Model v1.1, W3C, 2022, https://www.w3.org/TR/vc-data-model/.

[SLL20] Smith, B. et al.: On Credentials. Journal of Social Ontology 6/1, 2020.

[SO19] SOVRIN: On Guardianship in Self-Sovereign Identity, 2019, https://sovrin.org/wp-content/uploads/Guardianship-Whitepaper2.pdf.