5-11-2023

Beyond Paper and Plastic: A Meta-Model for Credential Use and Governance

Daniel Richter
HTW Dresden University of Applied Sciences, daniel.richter@htw-dresden.de

Christopher Robin Praas
HTW Dresden University of Applied Sciences, christopherrobin.praas@htw-dresden.de

Jürgen Anke
HTW Dresden University of Applied Sciences, juergen.anke@htw-dresden.de

BEYOND PAPER AND PLASTIC: A META-MODEL FOR CREDENTIAL USE AND GOVERNANCE

Complete Research

Richter, Daniel, HTW Dresden University of Applied Sciences, Dresden, Germany, daniel.richter@htw-dresden.de

Praas, Christopher Robin, HTW Dresden University of Applied Sciences, Dresden, Germany, christopher.praas@htw-dresden.de

Anke, Jürgen, HTW Dresden University of Applied Sciences, Dresden, Germany, juergen.anke@htw-dresden.de

Abstract

ID cards, public transport tickets, and diplomas are examples of credentials that society has established as a means to provide trustworthy information to others. In the digital world, the emergence of self-sovereign identity as a new paradigm for the management of digital credentials aims to narrow the conceptual gap between digital and physical credentials. The ongoing digital transformation in the public sector requires dealing with a large variety of credentials in different forms systematically. However, there is still currently no generic conceptual model of credentials in the Information Systems (IS) discipline. We employ design science research to develop a unified meta-model on credentials, their use, and their governance. Our results contribute to research through an empirically grounded conceptualization of credentials and provide practitioners with a common basis to capture, analyze, and design the handling of credentials in real-world scenarios.

Keywords: Credentials, Governance, Self-Sovereign Identity, Design Science Research.

1 Introduction

Credentials are documents that are used in almost every societal domain. The origin of these documents can often be found in the public sector. ID cards, driving licenses, and education certificates are examples of highly regulated credentials, which can be used across a variety of domains. Other credentials are integral to the functioning of the public sector itself, such as administrative decisions issued and reused by various authorities. Credentials can also be differentiated by the frequency of their use. While public transport tickets can be used daily, birth certificates, for example, are only used in key life events. As credentials play a central role in many areas of the public sector, we argue that its digital transformation depends on the provision of digital credentials. This can be observed in cases where otherwise digital processes are burdened by manual activities such as scanning or mailing documents (Heggertveit et al., 2022; Madsen, Lindgren, and Melin, 2022), or in-person verification (Lindgren, Madsen, et al., 2019). Thus, the digitization of credentials and the processes associated with their use bears large potentials for digital services in the public sector. In addition to user experience benefits, digital credentials are expected to support the creation of digital ecosystems by facilitating interorganizational data exchange (Laatikainen, Kolehmainen, and Abrahamsson, 2021). This is not only relevant for ecosystems such as smart cities, wherein administrations interact with various public and private actors to provide value

to citizens (Chourabi et al., 2012; Twizeyimana and Andersson, 2019), but also a maturity factor for e-government itself (Andersen and Henriksen, 2006).

National identification means (Shehu, Pinto, and Correia, 2019), electronic driving licenses (ISO, 2021), and electronic tickets (Mut-Puigserver et al., 2012) are some examples of currently used digital credentials in the public sector. These contemporary solutions, however, struggle to completely deliver on the above-mentioned benefits. Lacking a widespread standard for credentials of different types, service providers are challenged by the technical determinism for each additionally supported credential type (Bannister and Connolly, 2012). The lack of useful services in turn inhibits the acceptance by potential users (Carter et al., 2016).

Self-Sovereign Identity (SSI) is the latest approach in the development of digital credentials. It rests on a set of principles with the goal to empower users and to enable large-scale interoperability of digital credentials independent of their specific use case (Ferdous, Chowdhury, and Alassafi, 2019). In SSI, digital credentials are handled analogously to their physical counterparts: the issuance of credentials to user-controlled wallet applications is separated from their later use in specific service scenarios (Lacity and Carmel, 2022). Technical interoperability in SSI is achieved through a set of standards for identifiers, a credential data model as well as communication protocols (Davie et al., 2019).

The advent of SSI has renewed public interest in the digitization of credentials and led to the incubation of various development initiatives worldwide. A growing body of scientific literature guides these initiatives regarding technological and security aspects (Cucko and Turkanovic, 2021). However, recent IS research reports difficulties in practice based on pronounced conceptual gaps, calling for a more holistic understanding of credential use (Laatikainen, Kolehmainen, Li, et al., 2021). Part of these difficulties can be attributed to the dissonance of the various mental models resting on the multitude of already existing physical and digital credential implementations in practice (Laatikainen, Kolehmainen, and Abrahamsson, 2021). While working on a large cooperative research project on digital identities, we found that these diverging mental models make it hard to find a common language to discuss the specifics of digital credentials with researchers and practitioners.

Another recurring theme in these recent calls for research is a lack of knowledge on the governance of digital credentials (Sedlmeir et al., 2021). More specifically, IS practitioners are challenged by the development of rules and policies regulating the use of credentials (Laatikainen, Kolehmainen, and Abrahamsson, 2021). The importance of this aspect can be observed in a growing number of credential digitization projects. For instance, the former German federal government released a digital driver's license before the last general election in September 2021 (BMDV, 2021). The service was stopped shortly after (ADAC, 2022), in part due to unregulated verification processes, allowing for the transference of private data to potentially unauthorized parties (Wittmann, 2021). We argue that such challenges are connected to an insufficient conceptual understanding of credentials and their associated usage processes. In other words, it is hard to define rules and policies when it is not clear who or what is subject to these regulations. This confusion is further underlined by rapid technology trends introducing novel concepts and terminology.

As we have outlined, credentials are used in many areas of the public sector. These documents can differ substantially in their formats, intended uses, and regulatory requirements. In consequence, the digitization of credentials needs to account for these peculiarities. To allow for the mapping of this complexity of existing physical credentials to a specific technical implementation, a uniform way of description is necessary. In contrast, existing credential models either focus on specific types, use cases or technical approaches. Additionally, the governance aspect of credential use is largely unexplored, despite it being an important design challenge for credentials in the regulatory driven public sector. Based on these knowledge gaps, we state our research question:

"How can credentials, their use, and their governance be uniformly represented in a common model?"

To lay the foundation for a common understanding of credentials as a general IS phenomenon, we developed a meta-model of credential use and governance, synthesizing and abstracting from existing conceptualizations. For that development, we used an iterative design science research approach drawing

from established theory as well as practically relevant models on the use of credentials. The intended utility of the meta-model lies in aiding practitioners to analyze and describe existing credentials and to specify governance requirements for the development of new digital credentials by prescribing a set of related concepts and common terminology. To evaluate it for its efficacy, completeness, and consistency, we instantiated the meta-model multiple times during the design iterations using exemplary credential types from the public sector.
The remainder of this paper is structured as follows: In the next chapter, we analyze the background of our research in more detail. We present and discuss existing theoretical analyses of credentials as well as established practical approaches. Based on these, we derive the design requirements for the meta-model. Following that, we describe in chapter 3 the specific design science research approach employed in the development of the meta-model. The main part of the paper can be found in chapter 4 wherein we present an overview of the developed meta-model for credential use and governance. In the concluding chapters, we discuss the meta-model's validity, our contribution, and avenues for future research.

2 Background

In the introduction, we painted a colorful picture of various types of credentials without explicating or referring to a specific definition. The IS discipline so far has not proposed a conclusive conceptualization for this broad spectrum of documents. The focus on certain technological implementation approaches has led to conceptual confusion which we aim to relieve by abstracting the discussion to a meta-level. In this chapter, we present related work from IS research and practice as well as other disciplines which we used as a foundation for consolidation and abstraction. We further highlight the conceptual blank spots of each approach to derive the design requirements guiding the development of the meta-model presented and discussed afterward. Our analysis is conceptually not constrained to credentials but also includes the regulation of their use, i.e. the corresponding governance mechanisms.

2.1 Perspectives on digital credentials

In the IS discipline, theory on credentials as the main subject is rare. IS scholars so far have been more focused on **identity and access management (IAM)**. These efforts have produced a variety of approaches for IAM wherein credentials play only a subordinate role. This is because the emphasis in IAM lies on the specific decision processes of authentication and authorization (H. A. Smith and McKeen, 2011). While this perspective might be sufficient for organizations making such decisions based on certain presented credentials, it is discounting the remainder of their lifecycle. This has not emerged as a problem in IAM systems because of their underlying architectural considerations. In these systems, so-called identity providers are solely responsible for managing and providing user data to relying parties, i.e. applications a user wants to authenticate to (Zwattendorfer, Zefferer, and Stranacher, 2015). Users themselves only carry the responsibility of managing credentials as authentication means (Chadwick, 2009). The conceptual scope of this "managed" approach is insufficient to analyze the use of the wider array of credential types that are under the control of the user, i.e. most physical credentials. This is reflected in existing IAM meta-models, which do take credentials into account (Emig et al., 2007; Kern et al., 2004; Pohn and Hommel, 2022). The focus of these contributions, however, lies on describing technical architectures. The ontology of credentials and their governance mechanisms are largely out of scope. Policies play an important role in the meta-models by Emig et al. (2007) and Kern et al. (2004), but they describe the specific security requirements of relying parties, not the handling of credentials. Pohn and Hommel (2022) mention governance frameworks as a precondition for building trust in SSI-based systems, but they do not further specify their properties.
Privacy concerns (Crossler and Posey, 2017) and interoperability challenges (Jensen, 2012) of established IAM systems motivated the user-centric approach of **self-sovereign identity (SSI)**. Its basic principles were originally stated by Allen (2016) and have since then been discussed and refined by research and

practice (Schardong and Custódio, 2022). The guiding idea of SSI is to give users control over the handling of their owned data. This allows to design new interaction patterns in the digital world that mimic the exchange of physical credential documents (Grüner et al., 2020). In SSI, identity providers are replaced by so-called issuers, which issue credentials to the private wallet applications of so-called holders (Sartor et al., 2022). These can present their credentials independently of the corresponding issuers (hence self-sovereign) to relying parties, which in SSI are called verifiers (Mühle et al., 2018). To enable the interoperability of such a decentralized system, SSI rests heavily on a set of open standards. These include specifications for decentralized identifiers (Sporny, Longley, Sabadello, et al., 2022), data exchange protocols, and the verifiable credential (VC) data model (Sporny, Longley, and Chadwick, 2022). While the VC standard defines the data model of a specific type of digital credentials, i.e. VCs, it also offers insights into the conceptual considerations regarding the handling of credentials. This relevance is further emphasized by the fact that SSI builds on technology-agnostic principles, opening the path to a larger number of digital credential use cases beyond authentication and authorization. Beside the VC standard, in Liu et al. (2020) further analyses regarding the life cycle of credentials can be found. As the systematic mapping study by Cucko and Turkanovic (2021) shows, conceptual works in the area of SSI are rare and mostly focus on its guiding principles (Schardong and Custódio, 2022). Neither part of these principles nor of technical analyses consider the governance mechanisms for digital credential use, leading to the research gap illustrated in the introduction.

Originating in the discipline of Social Ontology, the **Theory of Document Acts (TDA)** (Koepsell and B. Smith, 2014; B. Smith, 2012, 2014) provides a framework for the conceptual analysis of credentials (B. Smith, Loddo, and Lorini, 2020). The main idea of TDA is that documents are not only used to record information but also to exercise certain powers with them. Credentials enable the exercising or denial of rights by acting as status indicators in a system of constitutive rules (Searle, 2005; B. Smith, Loddo, and Lorini, 2020). Therefore, any credential requires an accompanying governance regulating its intended use.

2.2 Approaches to credential governance

To standardize the technical architecture as well as to define a framework for governance in the SSI ecosystem the **Trust over IP (ToIP)** foundation was established as a Linux Foundation project. The key contribution to an understanding of credential governance made by the ToIP foundation is the so-called "ToIP stack", which consists of four layers. The first two layers describe identifier technology and communication protocols. Layer three specifies a role and life-cycle model for credential exchange, which is embedded in various application ecosystems at layer four (Davie et al., 2019). The ToIP stack recognizes that on each layer of technical infrastructure employed in SSI ecosystems distinct governance requirements can be found (Davie et al., 2019). The conceptual basis for the governance specifications in the ToIP stack is given by a meta-model specification that includes, among others, a governance framework document managed by a governing authority as well as governed parties (Trust Over IP Foundation, 2021b). The governance framework at layer three is a document consisting of "business, legal, and technical policies for issuing, holding, and verifying a set of credentials" (Trust Over IP Foundation, 2021a). Likewise, the governance framework on layer four regulates the application domains wherein the credentials are being used for various purposes. Governance on layer four can thus directly influence regulations on lower layers. As credentials are designed for a specific purpose, the differentiation between layers three and four is not always clear. Furthermore, the specifications by the ToIP foundation neither provide details on the nature of the relationships between governing authorities and governed parties nor on the contents of the policies regulating credential use. These ambiguities lead to difficulties in developing such policies and in identifying the relevant actors as shown by Laatikainen, Kolehmainen, and Abrahamsson (2021). A recent study by Sroor et al. (2022) with ToIP foundation members suggests beneficial effects of modeling in creating SSI governance frameworks, however without going into detail regarding the subjects of developed policies.

While not focusing specifically on credentials, the research stream on **information (technology) governance** can be identified in the IS discipline (Brown and Grant, 2005). Besides infrastructure and project management-related activities, the *use* of information technology is a key sphere for governance activities (Sambamurthy and Zmud, 1999). Tallon, Ramirez, and Short (2013) define this use "as a collection of capabilities or practices for the creation, capture, valuation, storage, usage, control, access, archival, and deletion of information over its life cycle." Likewise, Abraham, Schneider, and Vom Brocke (2019) highlight the importance of procedural governance mechanisms such as the definition of data standards and data policies "regarding the creation, acquisition, storage, security, quality, and permissible use of data". Similar considerations can be found in the e-government framework by Lindgren, Melin, and Sæbø (2021), which does not mention credentials specifically, but illustrates the important connection between information operations and the policies that shape this use. We derive from these works that a meta-model for credential governance requires an understanding of a credential's life cycle during its use by multiple actors.

2.3 Meta-model requirements

Physical and digital credentials of various types and differing technological foundations coexist in a variety of information systems. To design digital credentials, it is necessary to analyze existing and design new governance mechanisms, i.e. rules and policies. Such governance mechanisms should regulate the underlying standards and the use of credentials by specific actors in the credential's life cycle. IS research and practice, as well as other disciplines, use various conceptualizations of certain partial aspects of credential use and governance, often limited to specific technical architectures. This leads to the challenge of finding a common language when discussing credentials and specifying governance rules. We address these problems with a meta-model for credential use and governance. The corresponding requirements for such a meta-model are:

R1 Generic representation: The meta-model should abstract from specific credential use cases and employed technologies to allow a uniform description of the variety of physical and digital credentials in practice.

R2 Credential governance: The meta-model should allow to analyze, develop and communicate credential governance requirements.

R3 Credential use: The meta-model should be able to capture the life cycle of credentials by actors of varying roles as subjects governed by credential governance.

R4 Credential properties: The meta-model should be able to capture the properties of credentials that are relevant to their use and governance.

3 Method

Our research objective was to provide IS practitioners in credential digitization projects with a means to analyze, develop and communicate credential governance requirements. This utility is to be enabled by the use of a meta-model prescribing a structure of a set of relevant concepts. As the development of this artifact has been the main focus of our work we decided to use a design science research (DSR) approach (Hevner et al., 2004).

Brendel, Lembcke, and Kolbe (2022) developed a typology for classifying DSR projects along the axes of a) rigor versus relevance and b) instantiation versus theory. Our research falls into the *Designing* category of that typology as we find our research project a) in the highly relevant and dynamic environment of credential digitization and b) the nature of the developed meta-model is abstract in the sense that we are addressing a class of problems (credential governance) rather than a specific problem at hand.

For structuring our research process, we used the DSR methodology by Peffers et al. (2007). Furthermore, we used the guidelines by Hevner et al. (2004) to help identify the knowledge base as well as position our

research to its environment. The DSR approach as described by Peffers et al. (2007) consists of six steps, which allowed for an iterative development process of the meta-model during the objective definition, design, demonstration, and evaluation phases. An overview of our design process, the demonstration subjects as well as a selection of the main evaluation results of each cycle can be found in figure 1.

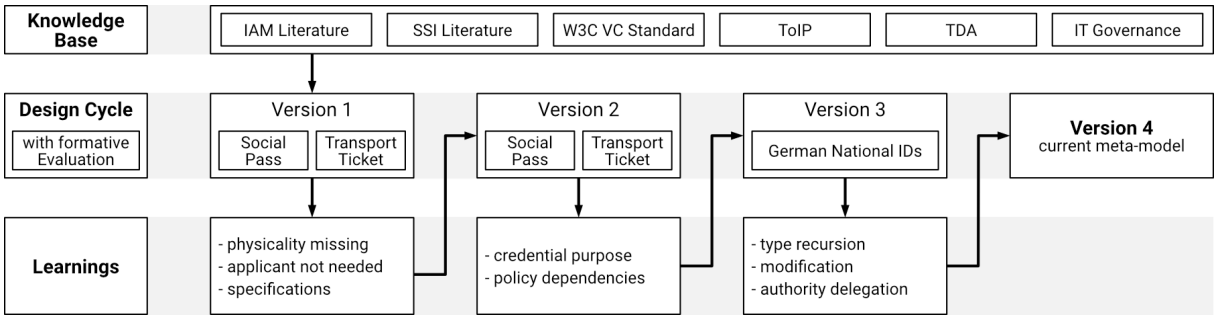

Figure 1. Meta-model design cycles.

The first version of the meta-model for credential use and governance was designed using the knowledge base as identified in chapter 2. During the design iterations, we applied problem-structuring and artifact design heuristics as presented in Gregory and Muntermann (2014). We split the meta-model into three main parts revolving around the credential construct: 1) credential properties, 2) credential use, and 3) credential governance. Based on these perspectives we scanned our knowledge base and started to model and relate the found constructs abstracting to fit the supposed generic nature of the meta-model. From this initial modeling, we arrived at the first stable version of the meta-model.

For the demonstration, we instantiated the meta-model by analyzing documents governing the use of relevant credentials from our knowledge base. This allowed us to contrast the efficacy of the meta-model across different contexts to improve its logical and empirical adequacy (Fisher and Aguinis, 2017). We purposefully chose physical credential types as demonstration subjects to show that the meta-model is not bound to a specific implementation approach even though we mainly used materials on digital credentials for its initial construction. For the first two demonstration cycles, we analyzed a municipal social pass issued by the social department of a large German city (over 550.000 residents) as well as a subscription-based public transport ticket from the same city. We had access to these two cases in the context of a German research project on secure digital identities.

As for the social pass, we found relevant governance information in a decree by the city government. Additionally, we carried out a semi-guided expert interview with the head of the social pass department to clarify our understanding of the regulation and to identify further policy practices not mentioned in the decree. For the public transport ticket, we used the terms and conditions of the regional transport association, information from the service website as well as the privacy policy of the issuing organization. Further, we contacted an IT manager of the public transport company regarding the verification practices of subcontractors, which were not explained in detail in the analyzed documents. In the third demonstration, we chose to analyze the German national identification means as regulated by federal law in the *Act on Identity Cards and Electronic Identification (Personalausweisgesetz)* and the corresponding ministerial *Identity Card Regulation (Personalausweisverordnung)*.

After each demonstration, we conducted an evaluation regarding the completeness (Hevner et al., 2004) of the meta-model with respect to the requirements R1-4 as stated in the previous section, as well regarding its consistency (Martin and Robertson, 2008). The evaluation phases resulted in sets of further requirements for the following design cycles regarding construct re-specification and the restructuring of relations (Fisher and Aguinis, 2017). Thus, the evaluations we conducted were formative for the design of the meta-model, which aligns with the guidelines by Venable, Pries-Heje, and Baskerville (2016) for more theoretical artifacts.

4 Artifact Description

Our meta-model consists of key constructs and their relationships. These constructs are represented with rectangular boxes of different colors and connected to each other by a unidirectional "has"-relationship. Table 1 describes the six element types and their corresponding representation in detail. The complete meta-model is presented in figure 2. It is organized into three main parts:

1. *Credential Properties:* The central part of the meta-model is comprised of the *credential* element and its corresponding properties. While the credential element refers to a concrete instantiated *document* the *credential type* is an abstraction thereof referring to a set of credentials. The rest of the meta-model structure results from these two levels of abstraction.

2. *Credential Use:* The top part of the meta-model from the credential element upwards describes the possible *operations* with a concrete credential by entities performing specific *roles*.

3. *Credential Governance:* The bottom part of the meta-model from the credential type element downwards describes the governance requirements connected to a credential type and thus only by extension to a set of credentials with that type. The light gray and yellow boxes in the background of figure 2 highlight how specific governance elements relate to their respective credential properties and operations.

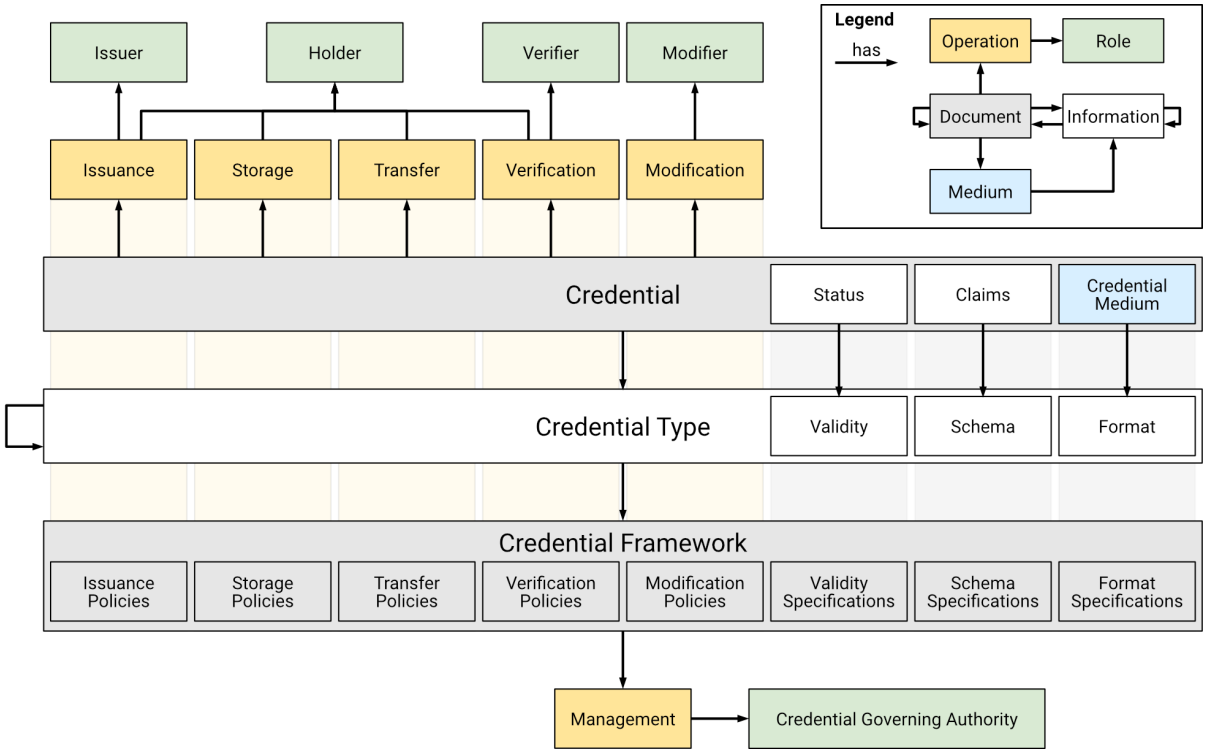

Figure 2. Graphical representation of the meta-model for credential use and governance.

In the following three sections we explain these parts one by one. We use a subscription-based ticket for public transport as an example, which is a plastic card with an integrated NFC chip as data storage. The ticket is paid on a monthly basis and has a minimum validity of one year.

Type	Representation	Description
Relation	Directed arrow, nested box	A relation connects an element unidirectionally to one or multiple other elements in a non-constitutive way.
Information	White box	Information are facts about someone or something.
Document	Gray box	A document consists of coherent pieces of information bound to a specific medium. A document can be interacted with by the means of operations.
Medium	Blue box	A medium is the representation of a document. For example a printed piece of paper, a plastic card, or an electronic matter on a device.
Operation	Yellow box	Operations allow interactions of entities with documents.
Role	Green box	A role is performed by an entity during an operation.

Table 1. Element types of the meta-model and their graphical representation.

4.1 Credential properties

Description: The base of our meta-model for credential use and governance is the credential itself. It has relations to other elements, but no other element "has" a credential. We define the credential as a document, which carries information and is bound to a *medium*. The information contains *claims* as well as a *status*. Claims are assertions about a subject, i.e. someone or something. The status shows the *validity* of the credential or gives a reference to where the validity of the credential can be checked. The medium is the actual representation of the credential and can be both physical and digital.

Every credential has a *credential type*. It contains information about the validity, the *schema*, and the *format* of one or multiple credentials. Validity is the fact of being able to be accepted or being acceptable by definition. The schema specifies the structure of the credential claims. The format describes the way in which information is arranged and stored. Credential types can be organized in hierarchies, i.e. a specific credential type can be derived from multiple more general types. Concrete credentials are instantiations of credential types.

Example: In our example a plastic card with an integrated NFC chip is the credential. Its credential type is "public transport ticket" with the superordinated type of "physical card with electronic storage". In contrast, another credential type could be a "mobile ticket" stored on a smartphone. The medium, our physical plastic card, contains certain claims which are declared by the schema in the credential type. This schema could include a card number as well as data like "passenger-type = adult" and "area of conduct = city". The format of the credential type states that the card is made of plastic, the card number is printed on the back side of the card, and all other information is stored on the NFC chip. In our NFC chip, we find the status "active and valid", which is one of the multiple states the credential can have, described in the validity of the credential type. Other states could be "inactive" and "active and revoked".

4.2 Credential use

Description: Starting from the credential in the previous section, we define that a credential has *operations*. An operation is an act of one or multiple actors with or to a credential. There are five operations in total occurring in a life cycle of a credential. In table 2 we give an overview of each operation and its definition. In each definition, we highlight the associated *roles* to that operation.

Operation	Definition
Issuance	. . . is an operation where the **issuer** makes claims about the credential's subject, creates a credential with informational contents, binds them to a medium and transfers the credential to its **holder**. Every credential has exactly one issuance.
Storage	. . . is an operation of the **holder** which describes the way a credential is bound to the holder's domain of control.
Transfer	. . . is an operation that describes the transmission of a credential from the **holder**'s domain to another holder. Losing a credential is a transfer to an unknown new holder, as its physical integrity and future use cannot be ruled out.
Verification	. . . is an operation comprising of a presentation of a credential from the **holder** to the **verifier**. Subsequently, the verifier inspects the credential regarding its validity according to a set of applicable governance regulations.
Modification	. . . is an operation carried out by a **modifier** which changes the credential's medium, information and/or status update. Destruction describes a form of modification, after which the credential ceases to exist.

Table 2. Operations and their definitions.

Based on the operations, we define five roles. In our meta-model, a role is understood as an entity which is corresponding to at least one operation. In the life cycle of a credential, an entity can take on different roles. However, the issuer cannot be changed after the issuance is done. In order to map complex structures in practice, we define that within every role, the actor can be delegated. For example, a natural person (employee) is in charge of certain tasks, like issuance and verification of a legal entity (company). Meaning that the issuer is still the company, while the actor is a human.
Example: Based on our public transport ticket, the transport company issues the tickets. However, a ticket can be obtained in multiple ways. One way would be, that the future holder, in this example an adult, requests a ticket in an online form, the transport company then checks the details and writes information on a card so the future holder can pick it up at a local service point. Another way would be that the ticket will be sent via mail after the request. After receiving the ticket, the holder can store it in their wallet with their personal belongings. The holder needs to take care of the ticket's integrity as it is not their property of them. A ticket can be transferred freely according to the subscription contract. The holder can therefore give the ticket to a friend, who becomes the ticket's new holder. While on a train, the holder is required to present the credential to the service personnel (verifier), who then proceeds to check the ticket electronically. If required, the service personnel can modify the ticket for example to reflect that it has been validated or that it has been revoked due to a missing payment from the holder. However, the holder itself could cut the card in half, which would also be a modification.

4.3 Credential governance

Description: The previously described use of credentials is governed through the definition and enforcement of a regulatory document we call *credential framework*. This framework is bound to the credential type and is therefore normative for all credentials of that type. As a credential type can refer to another credential type, multiple credential frameworks can influence the regulations of a single credential. A credential framework is managed by an entity with the role of *credential governing authority*. A credential governing authority has a certain legal authority in the scope of the credential's intended use and therefore also over the actors that carry out credential operations. The origin of this legal authority, e.g. by contract or by law, is outside the scope of this meta-model. The intended use of credentials of a type however needs to be defined in the credential framework, because the normative nature of the credential framework does not extend beyond that scope. As with every other role occurring in the meta-model an actor with the credential governing authority role may delegate a set of responsibilities to another actor. Likewise,

we acknowledge that a credential framework may be distributed over multiple disparate documents in practice. In the proposed design of the meta-model, we specify the credential framework into a set of eight non-constitutive sub-documents. These sub-documents can have one of two types:

1. *Specifications* are documents defining the set of valid properties of a credential type, i.e. validity, schema, and format. Specifications, therefore, establish which credentials are considered valid and genuine in the scope of the credential framework. In this sense, specifications are fixed as they are applicable independent of a specific operation.
2. *Policies* are documents governing the use of credentials of a type during the five operations. There is one policy type for each operation type: issuance, storage, transfer, verification, and modification. A policy of a specific type may regulate multiple instances of a single operation type. Policies may refer to the details defined in the specifications.

Example: In Germany, public transport is organized by regionally operating transport associations. These associations are formed by public transport businesses as well as municipal administrations of that region, dividing it into smaller tariff areas. The transport association acts as a governing authority for the transport tickets issued in the region. In our example, the complete credential framework for the subscription-based ticket is given by a number of different documents defined by at least four separate entities. The main regulatory contents are found in the terms and conditions of the transport association. In there, some parts of the regulation can be tied to all tickets issued in the region and some to the specific credential type that we focused on. We can observe for example the association-wide issuance policy that subscription-based tickets are issued in service centers. More details on the policies and specifications are provided through information on the website of the issuing transport business, which indicates a hierarchy of credential types. For example, an issuance policy for tickets issued by the local transport business defines that malfunctioning tickets are exchanged free of charge. A corresponding modification policy requires that all physical damages to the ticket shall be reported to the transport business. In order to prevent such damage, there is a storage policy, interestingly found on the privacy policy website of the transport business, stating that the tickets should not be put in contact with chemical solvents and be ideally kept in a dry space. An example of a transfer policy can be found on the website of the transport business which allows the transfer of the ticket for use by another person. Verification policies regulate the process of electronic ticket verification during the ride by the service personnel of a sub-contractor. The devices used by that personnel validate certain data fields in the chip of the ticket which is mostly nationally standardized by schema specifications maintained by the union of German transport associations (VDV, 2022). Whether the ticket is valid during the specific trip can be determined by the concrete manifestations of the data fields based on the validity policies of the transport business and the corresponding association's terms and conditions. Finally, the ticket's medium is designed after the format specifications as an NFC card compliant with the ISO/IEC 14443 standard (ISO, 2018).

5 Discussion

The heterogeneity of credentials in practice necessitates a uniform understanding of this general IS phenomenon, including its use and governance. Until now, there has been no conclusive model capturing this heterogeneity, leading to multiple challenges in the digital transformation of credentials. The developed meta-model supports this transformation process by providing an abstract view centered on the credential construct. In the following sections, we highlight how the developed meta-model contributes to both, theory and practice, what are its limitations, and present opportunities for further research.

5.1 Contributions to theory

As the credential construct has played only a subordinate role in the IS discipline, we have drawn from a variety of theoretical foundations in order to develop a common conceptual understanding of

credential properties, credential use, and credential governance. At the same time, we also contribute to this knowledge base through a generalized description of the phenomena that IAM, SSI, the ToIP framework, and the IT governance literature are focusing on.

Public sector theory in the IS discipline is enriched by our work in providing a detailed conceptualization of credentials and their accompanying regulations as distinct document types subjected to digitization efforts. This contribution is in line with other works focusing on the role of documents in e-government (Klischewski, 2006; Sourouni et al., 2008), such as forms (Scholta et al., 2020). The conceptualization we provided also details the interplay between information, its technologically-supported representation and corresponding regulation as highlighted by other conceptual works in e-government (Lindgren, Melin, and Sæbø, 2021, Janssen et al., 2020).

While the notion of a credential that we established in this contribution can hardly be recognized in IAM, we are adding to this research stream a more detailed view of regulations for the management of different authentication credentials. Furthermore, our credential-centric perspective on governance advances the understanding of security policies of relying parties in IAM meta-models (Emig et al., 2007; Kern et al., 2004; Pohn and Hommel, 2022), allowing for a more complete view of the origins of regulations.

The conceptual considerations in the scope of SSI provide a foundation for the modeling of the credential construct itself, especially regarding its informational contents (Sporny, Longley, and Chadwick, 2022), its lifecycle (Liu et al., 2020) as well as associated roles (Mühle et al., 2018). However, it does not contain the notion of a specific credential medium. By adding such medium and associated format properties we enable not only the analysis of physical credentials in the scope of the SSI principles (Allen, 2016) but also a more detailed discussion about various VC formats, which are present in practice (Young, 2021). Furthermore, we allow more fine-grained considerations on hierarchies of credential types by explicitly splitting a specific credential from that abstract type. While the lifecycle of credentials and the roles of issuer, holder, and verifier have been described already we add more dynamics to established SSI models by introducing the modification operation with the corresponding modifier role. This goes beyond the scope of a mere revocation and includes any changes to a credential's information or medium. Such cases are prominent in practice, and we thereby allow for an easier transformation of these into digital form by providing the foundation for analysis.

While already having generated awareness of its importance, SSI literature currently does not provide detailed insights into the governance of credentials. We combined the previously modeled credential properties and operations with ToIP's concept of a credential framework (Trust Over IP Foundation, 2021b) to conceptualize a set of five policies and three specifications regulating the use of credentials. These constructs are in line with the considerations on the governance of the lifecycle and fixed properties of data objects originating in the IT governance stream of the IS discipline. To this foundation, we add an understanding of how procedural governance mechanisms can be applied to data objects which are occurring in various digital and physical formats.

5.2 Contributions to practice

Credentials in various forms are relevant to many processes in the public sector. Digital transformation initiatives have to deal with a large variety of credentials, e.g. regarding their medium, content, and handling requirements. Additionally, the regulatory pressure for the proliferation of digital credentials in the public sector will likely increase. For example, the European Union (EU) regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) is currently in the process of major revisions. It is going to be utilizing key SSI concepts such as wallets and digital credentials (Sharif et al., 2022). In the future, public administrations in EU member states will need to be able to issue and verify so-called electronic attribute attestations, which at minimum are supposed to include, among others, qualifications, public permits and licenses, as well as financial and company data (European Commission, 2021).

Our proposed meta-model can support this transformation process through its application for the following purposes:

- Analysis of existing credentials and their governance, e.g. identification of gaps in their policies.
- Enable the efficient comparison of different credentials based on a common language as defined by the meta-model. This could also help new credential holders to better understand the rules and regulations.
- Support the design of new credentials, the continuous development of existing digital credentials, or the transformation of physical credentials into digital forms, which often cannot comply with the same policies.

These tasks can be supported through software tools for modeling the individual cases based on the meta-model. Developing such models may also serve the purpose of creating and maintaining structured documentation of credential governance, which can be exported in different formats. In the long term, this helps to create machine-readable governance to ensure the compliant handling of digital credentials across different domains automatically.

We found that the information we gathered information about policies and specifications is distributed over multiple separate documents or within a document. Some regulations were not documented at all but only lived in practice inherited. This diffusion of governance information may impede the digitization of physical credentials.

A big part of the complexity of our meta-model is probably due to primarily physical credentials. It is debatable whether all the special features of these credentials also have to be transferred to the digital world. However, since most regulatory frameworks relate primarily to physical credentials in administrative processes, it is necessary to systematically support the transformation of physical into digital credentials from a governance perspective. Our meta-model enables the systematic transformation of the variety of credentials in real-world applications.

5.3 Limitations

We developed a credential-centered meta-model for credential use and governance for both digital and physical credentials. While the presented model has been demonstrated with highly-relevant credential types from three distinct domains of the German public sector, there are likely advanced aspects that cannot yet be expressed properly. Examples include the handling of linked credentials, like car-sharing booking that depends on a valid driver's license, the life cycle of credentials with physical representation, e.g. preliminary identity cards, notarized documents such as certified copies of diplomas, or acting with credentials of third parties. A demonstration with a fully digital credential, without physical representation, as well as gathering feedback from potential users from multiple domains could give us new indications of aspects that may not yet be conveyed properly and could help in further broadening our conceptualization of credentials.

While credentials and their governance were the focus of this research, we acknowledge that more complexity resides in the use of credentials. This will be the scope of additional meta-models, which particularly aim to capture the acceptance of credentials using trust policies and the requirements of actors in specific ecosystems. The presented meta-model focuses mainly on the roles directly interacting with credentials. More detailed distinctions in the actor relationships such as guardianship or delegation were out of scope for the current version of the meta-model, since they depend on the specific applications of credentials in various scenarios.

A more detailed structuring of policies using dedicated modeling elements may be a promising approach to express references to credentials that are required for the issuing of another. Similarly, changing the status of one credential might influence the validity of others. Furthermore the meta-model currently only supports a single management operation with the credential framework document. As the lifecycle management of the underlying regulations might be quite complicated, especially in the public sector, a more detailed description could support maintaining the credential framework over time.

5.4 Future research

Our meta-model focuses on the perspective of a credential with its corresponding abstract type. Extensions of the meta-model on the level of the issuance and verification operations could allow for a more comprehensive analysis of the sum of requirements as well as the reasons for conducting credential exchange in real-world scenarios. While a public transport subscription might be used according to regulations found in the documents of the credential framework, this framework does not comprise all the trust policies and external requirements for the acceptance of such a ticket outside of the domain of public transport, e.g. for getting discounts with partner businesses. The use of credentials across these ToIP layer 4 application ecosystems, is common in practice and needs just as much attention as in their primary usage domains. This is where we see our work converging more with traditional analyses of security policies from the viewpoint of ecosystem actors, as opposed to credential roles. Likewise, the meta-model could be extended to allow for the description of the technical infrastructure for the exchange of credentials, making these comparable to the governance regulations of the current meta-model version. Apart from further extensions, we expect the current version of the meta-model to be used as a foundation for other artifacts. It could for example serve as a starting point to develop an abstract syntax for a domain-specific language for machine-readable governance. This could be a contribution to reaping the full benefits of automation in the verification of digital credentials. Other artifacts based on the meta-model could be a methodology for analyzing and designing credential governance as well as accompanying design principles.

6 Conclusion

Credentials play an important role in the public sector, co-existing in different physical and digital formats. Understanding and formulating governance requirements for credentials is thus a significant challenge in digital transformation projects. This is because credentials as a separate phenomenon have been under-addressed in IS research. We have found that the many technology-specific models existing do not capture the variety of credential representations and their use in practice. In this paper, we have presented a meta-model for credential use and governance which we developed during a DSR study grounded in both, established theory as well as multiple empirical demonstration subjects.

The presented meta-model contributes to practice as it allows to analyze, structure, define and communicate credential governance requirements in a common language. This helps to facilitate communication in digital transformation projects, e.g. when existing physical credentials are to be transformed into a digital representation. As the change of representation requires and enables a different handling, it is helpful to efficiently analyze and compare these different credentials and their governance.

Information systems theory is enriched by the presented meta-model by establishing credentials as a general phenomenon independent of a technological approach. We abstracted the theoretical foundations found in the realms of IAM and SSI, and integrated them with the established IS knowledge base on IT governance. It is however just the first step towards a more comprehensive theory of credentials in IS. In the future, we expect the design of further artifacts based on this meta-model, such as a methodology for analyzing and developing credential governance requirements. Opportunities for further theoretical advancements on credentials in IS are emerging in the direction of trust management and the acceptance of credentials across ecosystems.

Funding: The research project, on which this publication is based, was funded by the German Federal Ministry of Economic Affairs and Climate Action under grant number 01MN21001A.

References

Abraham, R., J. Schneider, and J. Vom Brocke (2019). "Data governance: A conceptual framework, structured review, and research agenda." *International Journal of Information Management* 49, 424–438. ISSN: 02684012. DOI: 10.1016/j.ijinfomgt.2019.07.008.

ADAC (2022). *Digitaler Führerschein: Nach wenigen Tagen gestoppt*. URL: https://www.adac.de/verkehr/rund-um-den-fuehrerschein/aktuelles/digitaler-fuehrerschein/ (visited on 11/17/2022).

Allen, C. (2016). *The Path to Self-Sovereign Identity*. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 11/16/2022).

Andersen, K. V. and H. Z. Henriksen (2006). "E-government maturity models: Extension of the Layne and Lee model." *Government Information Quarterly* 23 (2), 236–248. ISSN: 0740624X. DOI: 10.1016/j.giq.2005.11.008.

Bannister, F. and R. Connolly (2012). "Forward to the past: Lessons for the future of e-government from the story so far." *Information Polity* 17 (3,4), 211–226. ISSN: 15701255. DOI: 10.3233/IP-2012-000282.

BMDV (2021). *Technik für digitalen Führerschein steht*. Ed. by Bundesministerium für Digitales und Verkehr. URL: https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2021/114-scheuer-digitaler-fuehrerschein.html (visited on 11/17/2022).

Brendel, A. B., T.-B. Lembcke, and L. Kolbe (2022). "Towards an Integrative View on Design Science Research Genres, Strategies, and Pivotal Concepts in Information Systems Research." *Data Base for Advances in Information Systems*.

Brown, A. E. and G. G. Grant (2005). "Framing the Frameworks: A Review of IT Governance Research." *Communications of the Association for Information Systems* 15. DOI: 10.17705/1CAIS.01538.

Carter, L., V. Weerakkody, B. Phillips, and Y. K. Dwivedi (2016). "Citizen Adoption of E-Government Services: Exploring Citizen Perceptions of Online Services in the U." *Information Systems Management* 33 (2), 124–140. DOI: \url{10.1080/10580530.2016.1155948}.

Chadwick, D. W. (2009). "Federated Identity Management." In: *Foundations of Security Analysis and Design V*. Ed. by A. Aldini, G. Barthe, and R. Gorrieri. Vol. 5705. Lecture notes in computer science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 96–120. ISBN: 978-3-642-03828-0. DOI: 10.1007/978-3-642-03829-7_3.

Chourabi, H., T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, and H. J. Scholl (2012). "Understanding Smart Cities: An Integrative Framework." In: *2012 45th Hawaii International Conference on System Sciences*. IEEE, pp. 2289–2297. ISBN: 978-1-4577-1925-7. DOI: 10.1109/HICSS.2012.615.

Crossler, R. and C. Posey (2017). "Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem." *Journal of the Association for Information Systems* 18 (7). DOI: 10.17705/1jais.00463.

Cucko, S. and M. Turkanovic (2021). "Decentralized and Self-Sovereign Identity: Systematic Mapping Study." *IEEE Access* 9, 139009–139027. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3117588.

Davie, M., D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, and D. Reed (2019). "The Trust over IP Stack." *IEEE Communications Standards Magazine* 3 (4), 46–51. ISSN: 2471-2825. DOI: 10.1109/MCOMSTD.001.1900029.

Emig, C., F. Brandt, S. Abeck, J. Biermann, and H. Klarl (2007). "An Access Control Metamodel for Web Service-Oriented Architecture." In: *International Conference on Software Engineering Advances (ICSEA 2007)*. IEEE, p. 57. ISBN: 0-7695-2937-2/07. DOI: 10.1109/ICSEA.2007.15. URL: http://ieeexplore.ieee.org/servlet/opac?punumber=4299876.

European Commission (June 2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework*

for a European Digital Identity. Brussels. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN (visited on 03/28/2023).

Ferdous, M. S., F. Chowdhury, and M. O. Alassafi (2019). "In Search of Self-Sovereign Identity Leveraging Blockchain Technology." *IEEE Access* 7, 103059–103079. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2931173.

Fisher, G. and H. Aguinis (2017). "Using Theory Elaboration to Make Theoretical Advancements." *Organizational Research Methods* 20 (3), 438–464. ISSN: 1094-4281. DOI: 10.1177/1094428116689707.

Gregory, R. W. and J. Muntermann (2014). "Research Note: Heuristic Theorizing: Proactively Generating Design Theories." *Information Systems Research* 25 (3), 639–653. DOI: 10.1287/isre.2014.0533. URL: https://www.jstor.org/stable/24700315.

Grüner, A., A. Mühle, T. Gayvoronskaya, and C. Meinel (2020). "A Comparative Analysis of Trust Requirements in Decentralized Identity Management." In: *Advanced information networking and applications*. Ed. by L. Barolli, T. Enokido, M. Takizawa, and F. Xhafa. Vol. 926. Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, pp. 200–213. ISBN: 978-3-030-15031-0. DOI: 10.1007/978-3-030-15032-7_18.

Heggertveit, I., I. Lindgren, C. Ø. Madsen, and S. Hofmann (2022). "Administrative Burden in Digital Self-service: An Empirical Study About Citizens in Need of Financial Assistance." In: *Electronic Participation*. Ed. by R. Krimmer, M. Rohde Johannessen, T. Lampoltshammer, I. Lindgren, P. Parycek, G. Schwabe, and J. Ubacht. Vol. 13392. Lecture notes in computer science. Cham: Springer Nature Switzerland, pp. 173–187. ISBN: 978-3-031-23212-1. DOI: 10.1007/978-3-031-23213-8{\textunderscore}11.

Hevner, A. R., S. T. March, J. Park, and S. Ram (2004). "Design Science in Information Systems Research." *MIS Quarterly* 28 (1), 75–105. ISSN: 02767783. URL: https://www.jstor.org/stable/25148625.

ISO (2018). *ISO/IEC 14443-1:2018: Cards and security devices for personal identification — Contactless proximity objects —– Part 1: Physical characteristics*. Geneva, Switzerland. URL: https://www.iso.org/standard/73596.html.

— (2021). *ISO/IEC 18013-5:2021: Personal identification — ISO-compliant driving licence —– Part 5: Mobile driving licence (mDL) application*. Geneva, Switzerland. URL: https://www.iso.org/standard/69084.html.

Janssen, M., P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski (2020). "Data governance: Organizing data for trustworthy Artificial Intelligence." *Government Information Quarterly* 37 (3), 101493. ISSN: 0740624X. DOI: 10.1016/j.giq.2020.101493.

Jensen, J. (2012). "Federated Identity Management Challenges." In: *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, pp. 230–235. ISBN: 978-1-4673-2244-7. DOI: 10.1109/ARES.2012.68.

Kern, A., M. Kuhlmann, R. Kuropka, and A. Ruthert (2004). "A meta model for authorisations in application security systems and their integration into RBAC administration." In: *Proceedings of the ninth ACM symposium on Access control models and technologies - SACMAT '04*. Ed. by T. Jaeger and E. Ferrari. New York, New York, USA: ACM Press, p. 87. ISBN: 1581138725. DOI: 10.1145/990036.990050.

Klischewski, R. (2006). "Ontologies for e–document management in public administration." *Business Process Management Journal* 12 (1), 34–47. ISSN: 1463-7154. DOI: 10.1108/14637150610643742.

Koepsell, D. and B. Smith (2014). "Beyond Paper." *The Monist* 97 (2), 222–235. DOI: 10.5840/monist201497215.

Laatikainen, G., T. Kolehmainen, and P. Abrahamsson (2021). "Self-Sovereign Identity Ecosystems: Benefits and Challenges." In: *12th Scandinavian Conference on Information Systems*. Orkanger, Norway: Association for Information Systems. URL: https://aisel.aisnet.org/scis2021/10/.

Laatikainen, G., T. Kolehmainen, M. Li, M. Hautala, and A. Kettunen (2021). "Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems." In: *Twenty-fifth Pacific Asia Conference on Information Systems*. Dubai, UAE: Association for Information Systems. ISBN: 978-1-7336325-7-7.

Lacity, M. and E. Carmel (2022). "Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet." *MIS Quarterly Executive* 21 (3), 241–251. URL: https://aisel.aisnet.org/misqe/vol21/iss3/6.

Lindgren, I., C. Ø. Madsen, S. Hofmann, and U. Melin (2019). "Close encounters of the digital kind: A research agenda for the digitalization of public services." *Government Information Quarterly* 36 (3), 427–436. ISSN: 0740624X. DOI: 10.1016/j.giq.2019.03.002.

Lindgren, I., U. Melin, and Ø. Sæbø (2021). "What is E-Government? Introducing a Work System Framework for Understanding E-Government." *Communications of the Association for Information Systems* 48. DOI: 10.17705/1CAIS.04842.

Liu, Y., Q. Lu, H.-Y. Paik, and X. Xu (2020). "Design Patterns for Blockchain-based Self-Sovereign Identity." In: *Proceedings of the European Conference on Pattern Languages of Programs 2020*. ACM Digital Library. New York,NY,United States: Association for Computing Machinery, pp. 1–14. ISBN: 9781450377690. DOI: 10.1145/3424771.3424802.

Madsen, C. Ø., I. Lindgren, and U. Melin (2022). "The accidental caseworker – How digital self-service influences citizens' administrative burden." *Government Information Quarterly* 39 (1), 101653. ISSN: 0740624X. DOI: 10.1016/j.giq.2021.101653.

Martin, R. and E. Robertson (2008). ""Meta" Matters." In: *CONF-IRM 2008 Proceedings*. Association for Information Systems, p. 1. URL: https://aisel.aisnet.org/confirm2008/1.

Mühle, A., A. Grüner, T. Gayvoronskaya, and C. Meinel (2018). "A Survey on Essential Components of a Self-Sovereign Identity." In: *Computer Science Review*. Vol. 30, pp. 80–86. DOI: 10.1016/j.cosrev.2018.10.002.

Mut-Puigserver, M., Payeras-Capellà, M. Magdalena, Ferrer-Gomila, Josep-Lluís, Vives-Guasch, Arnau, and J. Castellà-Roca (2012). "A survey of electronic ticketing applied to transport." *Computers & Security* 31 (8), 925–939. ISSN: 0167-4048. DOI: 10.1016/j.cose.2012.07.004. URL: https://www.sciencedirect.com/science/article/pii/S0167404812001058.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee (2007). "A Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems* 24 (3), 45–77. DOI: 10.2753/MIS0742-1222240302.

Pohn, D. and W. Hommel (2022). "Reference Service Model Framework for Identity Management." *IEEE Access*, 1. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3219044.

Sambamurthy, V. and R. Zmud (1999). "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies." *MIS Quarterly* 23 (2), 261–290. ISSN: 02767783.

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

Schardong, F. and R. Custódio (2022). "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy." *Sensors* 22 (15). ISSN: 1424-8220. DOI: 10.3390/s22155641. URL: https://www.mdpi.com/1424-8220/22/15/5641.

Scholta, H., D. Balta, M. Räckers, J. Becker, and H. Krcmar (2020). "Standardization of Forms in Governments." *Business & Information Systems Engineering* 62 (6), 535–560. ISSN: 2363-7005. DOI: 10.1007/s12599-019-00623-1.

Searle, J. R. (2005). "What is an institution?" *Journal of Institutional Economics* 1 (1), 1–22. ISSN: 1744-1374. DOI: 10.1017/S1744137405000020.

Sedlmeir, J., R. Smethurst, A. Rieger, and G. Fridgen (2021). "Digital Identities and Verifiable Credentials." *Business & Information Systems Engineering*. ISSN: 2363-7005. DOI: 10.1007/s12599-021-00722-y.

Sharif, A., M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, and S. Ranise (2022). "The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." *applied sciences* 12. DOI: 10.3390/app122412679.

Shehu, A.-s., A. Pinto, and M. E. Correia (2019). "On the Interoperability of European National Identity Cards." In: *Ambient Intelligence – Software and Applications –, 9th International Symposium on Ambient Intelligence*. Ed. by P. Novais, J. J. Jung, G. Villarrubia González, A. Fernández-Caballero, E. Navarro, P. González, D. Carneiro, A. Pinto, A. T. Campbell, and D. Durães. Cham: Springer International Publishing, pp. 338–348. ISBN: 978-3-030-01746-0.

Smith, B. (2012). "How to Do Things with Documents." *Rivista di estetica* (50), 179–198. ISSN: 0035-6212. DOI: 10.4000/estetica.1480.

— (2014). "Document Acts." In: *Institutions, Emotions, and Group Agents*. Ed. by A. Konzelmann Ziv and H. B. Schmid. Dordrecht: Springer Netherlands, pp. 19–31. ISBN: 978-94-007-6933-5. DOI: 10.1007/978-94-007-6934-2_2.

Smith, B., O. G. Loddo, and G. Lorini (2020). "On Credentials." *Journal of Social Ontology* 6 (1), 47–67. ISSN: 2196-9655. DOI: 10.1515/jso-2019-0034.

Smith, H. A. and J. D. McKeen (2011). "The Identity Management Challenge." *Communications of the Association for Information Systems* 28. DOI: 10.17705/1CAIS.02811.

Sourouni, A.-M., F. Lampathaki, S. Mouzakitis, Y. Charalabidis, and D. Askounis (2008). "Paving the Way to eGovernment Transformation: Interoperability Registry Infrastructure Development." In: *Electronic government*. Lecture notes in computer science. Berlin: Springer, pp. 340–351. ISBN: 9783540852049.

Sporny, M., D. Longley, and D. W. Chadwick (2022). *Verifiable Credentials Data Model v1.1: W3C Recommendation*. Ed. by M. Sporny, G. Noble, D. Longley, D. Burnett, B. Zundel, and K. den Hartog. URL: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/ (visited on 11/16/2022).

Sporny, M., D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen (2022). *Decentralized Identifiers (DIDs) v1.0: W3C Recommendation*. Ed. by M. Sporny, A. Guy, M. Sabadello, and D. Reed. URL: https://www.w3.org/TR/2022/REC-did-core-20220719/ (visited on 11/17/2022).

Sroor, M., N. Hickman, T. Kolehmainen, G. Laatikainen, and P. Abrahamsson (2022). "How modeling helps in developing self-sovereign identity governance framework: An experience report." *Procedia Computer Science* 204, 267–277. ISSN: 18770509. DOI: 10.1016/j.procs.2022.08.032.

Tallon, P. P., R. V. Ramirez, and J. E. Short (2013). "The Information Artifact in IT Governance: Toward a Theory of Information Governance." *Journal of Management Information Systems* 30 (3), 141–178. DOI: 10.2753/MIS0742-1222300306.

Trust Over IP Foundation (Nov. 2021a). *Introduction to Trust Over IP. Version 2.0*. URL: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf (visited on 11/10/2022).

— (Dec. 2021b). *ToIP Governance Metamodel Specification. Version 1.0*. URL: https://trustoverip.org/wp-content/uploads/ToIP-Governance-Metamodel-Specification-V1.0-2021-12-21.pdf (visited on 11/10/2022).

Twizeyimana, J. D. and A. Andersson (2019). "The public value of E-Government – A literature review." *Government Information Quarterly* 36 (2), 167–178. ISSN: 0740624X. DOI: 10.1016/j.giq.2019.01.001.

VDV (2022). *VDV-KA and (((etiCORE / VDV eTicket Service*. Ed. by VDV eTicket Service GmbH & Co. KG. Cologne, Germany. URL: https://www.eticket-deutschland.de/en/eticket/ticketing-standards (visited on 11/16/2022).

Venable, J., J. Pries-Heje, and R. Baskerville (2016). "FEDS: a Framework for Evaluation in Design Science Research." *European Journal of Information Systems* 25 (1), 77–89. DOI: 10.1057/ejis.2014.36.

Wittmann, L. (2021). *Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen.* URL: https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-

und-jeder-sein-au%7B%5Css%7Der-du-musst-dich-ausweisen-829293739fa0 (visited on 11/17/2022).

Young, K. (2021). *Verifiable Credentials Flavors Explained*. Ed. by Linux Foundation Public Health. URL: https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf (visited on 11/17/2022).

Zwattendorfer, B., T. Zefferer, and K. Stranacher (2015). "A Comparative Survey of Cloud Identity Management-Models." In: *Web Information Systems and Technologies*. Ed. by V. Monfort and K.-H. Krempels. Cham: Springer International Publishing, pp. 128–144. ISBN: 978-3-319-27030-2.