Electronic Markets (2023) 33:3
https://doi.org/10.1007/s12525-023-00620-z

RESEARCH PAPER

Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes

Tobias Guggenberger[1,2,3] · **Daniela Kühne**[4] · **Vincent Schlatt**[2] · **Nils Urbach**[1,2,5]

Received: 23 January 2022 / Accepted: 27 February 2023 / Published online: 15 April 2023

Abstract

The introduction of blockchain offers new opportunities to rethink enterprise identity management. Recently, a new concept has emerged in the blockchain community called self-sovereign identity. Self-sovereign identity combines several existing decentralized identity management approaches, promising new ways to promote more convenient, connected, and secure identity services for the private and public sector. Nevertheless, research in this area is still in its infancy. Most of the very few articles focus either on the opportunities self-sovereign identity might offer or on very specific technical features. Studies on real-world applications of organizations using modern self-sovereign identity implementations and design theory are very rare. To fill this gap, we follow the design science research approach to design, implement, and evaluate a self-sovereign identity system to present tax attributes of online retailers. We present four design principles and conclude that the use of self-sovereign identity and blockchain offers opportunities to improve verification processes.

Keywords Blockchain · Identity management · Self-sovereign identity · Public sector · eIDAS · Digital wallet

JEL Classification O33

Introduction

On September 17, 2014, the regulation on identification and trust services for electronic transactions in the internal market (eIDAS) entered into force. The European Union adopted eIDAS to create a framework for secure and reliable electronic identification and trust services that ensure cross-border interoperability and provide citizens and businesses with secure and easy-to-use online interactions with public and private services. (European Commission, 2021). Since its implementation in 2017, eIDAS has established a foundation for digital identities in Europe and has been used as the basis for many e-government services (EUR-Lex, 2014). Despite promising secure and supposedly easy-to-use ways to provide electronic identification, only 14 of the 28 member states of the European Union have adopted an electronic identity (eID) in line with the regulation. Taking a closer look at the national level, the adoption of eID services provided by the government is very low. As the most notable example, only 7% of German Citizens have used the German eID so far (European Commission, 2021).

In 2020, the European Commission launched a study investigating why countries in Europe do not adopt digital identities (European Commission, 2020). The report concluded that the existing European identity network does not meet the changing demands for digital identities. It explicitly addresses the fact that the current technical implementation reveals weaknesses. First and foremost, the data set in the current implementation of eIDAS is severely limited

Responsible Editor: Andreas Hein.

✉ Tobias Guggenberger
tobias.guggenberger@fim-rc.de

Daniela Kühne
daniela.kuehne@lfst.bayern.de

Vincent Schlatt
vincent.schlatt@fim-rc.de

Nils Urbach
nils.urbach@fb3.fra-uas.de

[1] Branch Business & Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany

[2] Research Center Finance & Information Management, Bayreuth, Germany

[3] University of Bayreuth, Bayreuth, Germany

[4] Bavarian State Tax Office, Munich, Germany

[5] Frankfurt University of Applied Sciences, Frankfurt, Germany

and focuses only on the master data of private individuals. Such master data typically comprises core information, e.g., name, address, date of birth, and national identification number. Therefore, additional attributes (e.g., tax attributes, degree of education) and legal entities are currently not covered. In addition, the current system, designed primarily for e-government, limits its use for businesses, resulting in minimal integration of the public and private sectors (European Commission, 2020).

To overcome these limitations, the European Union is working towards a new, European-wide identity network called eIDAS 2.0. This system aims to improve upon the current identity management infrastructure by facilitating the exchange of identity data between public institutions and private companies (European Commission, 2021). One of the key concepts being considered as the foundation for eIDAS 2.0 is self-sovereign identity (SSI) (European Commission, 2021; Preukschat, 2021). SSI is an approach that utilizes blockchain technology to give individuals more control over their own identity data (Wang & Filippi, 2020). By using decentralized identifiers and modern cryptography, eIDAS 2.0 aims to improve privacy and security while making it easier for citizens and also businesses to access a wide range of digital services. This is a significant departure from the current eIDAS infrastructure, which was primarily designed for citizens and the public sector (European Commission, 2021). With SSI, any type of attestation can be represented, opening up new possibilities for the use of digital identities.

Despite its potential benefits, the high costs of implementation and operation of SSI present a challenge and hinder its widespread adoption by the public and private sectors. The initial setup of a new SSI-based pan-European IdM alone is estimated to cost more than 600 million euros, plus the operating costs for public and private organizations during the period of use (European Commission, 2021). Most of the very few research articles on SSI that could help make informed decisions in this area of tensions either focus on the hypothetical opportunities the paradigm has for society in general or on specific technical particularities (Liu et al., 2020). And even though research on blockchain-based IdM generally exists that could provide a first foundation (Dunphy & Petitcolas, 2018; Faber et al., 2019; Sullivan & Burger, 2017), they do not cover all particularities of modern SSI implementations, such as ZKP, accumulators, and the employed standards and how they manifest in business cases.

Due to its complexity, designing effective information systems based on SSI requires a deep understanding of the various use cases and the needs of different stakeholders (Nærland et al., 2017; Treiblmaier & Beck, 2019). Only then can we ensure that the system achieves the necessary privacy, security, interoperability, and scalability. Nevertheless, the theory of SSI system design is still largely undiscovered, resulting in difficulties for organizations, such as government institutions and companies, to fully leverage the potential benefits of SSI systems (Preukschat, 2021; Zhu & Badr, 2018). To bridge this gap in research, we ask the following question:

> RQ: How can blockchain-based SSI be incorporated for decentralized identity management spanning multiple organizations?

To answer this question, we follow the design science research (DSR) paradigm to ensure rigor and generalizability throughout our research (Gregor & Hevner, 2013; Peffers et al., 2007). In particular, we present an SSI system that allows online retailers to retain multiple Verifiable Credentials (VC) to prove the proper registration as a taxpayer against an online platform (e.g., Amazon, eBay). We chose this use case as a perusing example because (1) existing solutions within this field face typical problems like counterfeiting, privacy issues, and inefficiencies, (2) the use case involves an identity holder that transacts with multiple certificate issuing authorities and verifiers spanning across various organizations, and (3) the incorporated parties involve public institutions as well as private companies demonstrating the ecosystem characteristics of SSI. Therefore, we aim to design and implement an SSI system that replaces the existing paper-based application.

Besides presenting and evaluating the final solution design, we derive four nascent design principles (Baskerville et al., 2018), which we present in the discussion section of this article. The principles are (1) *Utilize the multiplicity of roles of actors for scaling the identity ecosystem:* SSI provides means for actors to engage in different roles, which greatly improves scalability in comparison to eIDAS, where roles are strictly tied to entities. (2) *Consider credentials for multiple applications to facilitate additional use cases:* With SSI, credentials are not bound to specific use cases, demonstrating the multipurpose nature of the paradigm spanning both applications within the public and private industry. (3) *Recognize the identity holder as the primary controller to ensure seamless processes:* SSI is highly user-centric, which means that all processes have to involve the user and are mostly bilateral. Therefore, third parties cannot track the activities of the identity holder. Finally, (4) *Use Public DIDs only for credential issuers to minimize privacy issues:* SSI typically uses blockchain in contrast to eIDAS. To still provide privacy, identifiers should only be used by parties who intend to issue credentials.

This study contributes to the field of e-government systems and the broader field of identity management in several key ways. Firstly, it provides practical insights into the design and underlying decisions of SSI systems, giving guidance for organizations and institutions looking to implement

similar systems. This includes both government institutions and private companies. Secondly, by evaluating the design and implementation of SSI, we shed light on the strengths and weaknesses of this approach. These findings provide valuable insights for any organization looking to adopt SSI and understand the potential benefits and challenges associated with the technology. For example, organizations considering use cases with a high demand for audits may face challenges in executing these with an SSI system. Thirdly, the study provides design principles as guidelines for SSI and blockchain-based identity management systems, contributing to the broader design theory beyond the specific use case. This aligns with the call for guidelines in previous studies (Carter & Ubacht, 2018; Nærland et al., 2017) and can help organizations and institutions to optimize their SSI systems and ensure they meet the needs of all stakeholders.

Related work

Centralized and federated identity management systems

The extensive use of digital identities characterizes our digital, interconnected society. Many digital services in our personal and professional life require identification and identity verification (Cao & Yang, 2010). For handling the identities of their customers and employees, organizations use IdMs. These systems are paramount for the administration of digital identities along the identity lifecycle, which includes the issuance, updating, and revocation of identities (Clauß & Köhntopp, 2001). Thus, they provide an often necessary foundation for trust in digital transaction relationships on electronic markets (Cao & Yang, 2010; Clauß & Köhntopp, 2001).

Various forms of IdMs have been developed, of which centralized and federated are the most used ones. In a centralized IdM, a user creates an identity in the system by registering an account with an application, typically providing a username and a password (Preukschat, 2021). While such systems are very simple to implement, they also show deficits, e.g., accounts are typically only valid for a single application. Thus, identity information is not transferable, resulting in additional efforts for the user and lacking interoperability between applications (Zhu & Badr, 2018).

Federated IdMs try to improve over centralized IdMs. Instead of creating an account directly with an application provider, the user registers at an identity provider. When the user accesses an application, the IDP relays a portion of their identity information to this application (Zhu & Badr, 2018). One of the largest federated IdMs is the European eID, governed under the eIDAS regulation, aiming to serve almost 500 million people. The system uses a network of eIDAS Nodes, which are run by national governments and act as identity providers for their citizens. Service providers, such as government websites, can then use these eIDAS Nodes to identify and authenticate users. This allows citizens to use their own national eID to access services in their own and other European countries (Carretero et al., 2018).

Despite their benefits, federated IdMs still come with their drawbacks (Jensen, 2012). One major concern is the presence of intermediaries between users and service providers, which can lead to privacy issues and the potential tracking of citizens and companies (Squicciarini et al., 2008). Because information passes through the identity provider, they could potentially use this as a means to (partially) track the activities of identity holders. Additionally, onboarding of new identity providers within a federation can be complex and costly, making it difficult for new entities to join the network or for existing entities to expand their participation (Jensen, 2012). To address these issues, decentralized approaches for IdM services are currently being researched and considered as an alternative solution.

Blockchain-based identity management systems

Due to the ever-growing digitalization, an increasing number of digital identities and systems must be managed (Caza et al., 2018). In conjunction with the rising interest in blockchain (Arnold et al., 2019), researchers started to rethink existing IdM paradigms. Blockchain's characteristics, e.g., decentralization, interoperability, and high level of security (Guggenberger et al., 2020), promise to offer opportunities to improve existing IdM systems providing means to transition from centralized and federated IdMs to decentralized IdMs (Lesavre, 2020; Sourabh, 2019; Zambrano et al., 2018).

Several researchers have analyzed how blockchain-based IdMs can benefit institutions and users alike (Liu et al., 2020). Since typically public institutions issue trustworthy digital identities, an important research strand has emerged around corresponding e-government solutions. For example, Sullivan and Burger (2017) describe a technical implementation of a blockchain-based IdM to represent the Estonia e-ID. The authors point out that blockchain "could fundamentally change the way identity information is controlled and authenticated" (Sullivan & Burger, 2017). The system facilitates improved control of citizens over their identity by allowing them to use the blockchain to define which property is shared with whom granularly. Faber et al. (2019) followed a similar approach to incorporate blockchain to create a GDPR-compliant IdM system. The authors argue that blockchain provides high security, trust, and transparency. Ultimately, their system enables users to control their data, shifting the power to the end users. Besides master identity information, IdM systems can also provide evidence

of more specific properties. The representation of diplomas is a well-analyzed use case for blockchain-based IdM, and even systems for the management of diplomas already exist (Marina et al., 2020). Table 1 illustrates our literature review and summarizes existing research in the context of IdM and e-government. For a more holistic overview of blockchain-based IdMs beyond the e-government sector, we would like to refer to the systematic literature review of Rathee and Singh (2021).

In summary, researchers present that blockchain offers opportunities to improve IdM in the e-government sector. Nevertheless, as our literature review shows, most designs still do not use interoperable standards, advanced cryptography, and certificates. Instead, previous research uses proprietary solutions that typically combine smart contracts and off-chain repositories (centralized servers or IPFS). Only Gao et al. (2018) provide insights into how certificates stored on user devices can be employed with blockchain.

Against this background, SSI has emerged as a new concept from the blockchain community. SSI combines several existing approaches of other decentralized IdM, such as ZKP, decentralized public key infrastructure, certificates, and blockchain, to provide a comprehensive framework to manage identities (Preukschat, 2021).

Conceptual foundations of self-sovereign identity

Preukschat (2021) describes SSI as a concept in which the identity of a user is "neither dependent on nor subject to any other power or state" (Preukschat, 2021). At the core of the SSI concept is the belief that the user should be the owner and have full control over their identity (Allen, 2016). Nevertheless, it is important to note that the field of SSI is diverse and dynamic, and there are multiple interpretations and conceptualizations of what exactly constitutes SSI. Despite this, the core principle of user control and ownership remains consistent across all interpretations (Der et al., 2017; Mühle et al., 2018; Wang & Filippi, 2020).

For the sake of this study, we primarily adhere to the conceptualization of Preukschat (2021) and the W3C (2021a). As depicted in Fig. 1, the typical building blocks of such an SSI system are Verifiable Credentials (VC) and Verifiable Presentations (VP), wallets, Decentralized Identifiers (DID), and a Verifiable Data Registry, commonly represented by a blockchain (Mühle et al., 2018).

VCs build the operational component representing identity attributes. VCs are cryptographically signed digital objects which allow holders to make claims about themselves. VCs are similar to digitally signed certificates but are never meant to be shown directly to a verifier. Instead, the VC holder creates VPs, which are tamper-proof presentations of evidence that the user can derive from one or multiple VCs. Such evidence includes properties themselves, the issuer's signature, and proof that the VC has not been revoked. VCs also support the use of cryptographic ZKP to minimize data disclosure. As such, it is possible, e.g., that a user can prove only some properties of a VC or that they are older than a certain age limit without revealing their exact age (Mühle et al., 2018).

Over time, identity holders accumulate a wide variety of different VCs. Therefore, it is necessary to provide secure and convenient means for users to manage all their VCs and interactions with other parties. Like a purse where we collect our official documents, SSI uses *digital wallets* to manage VCs, digital keys, VP creation, and connections to issuers and verifiers. Depending on the characteristics of an identity holder, they can use different forms of wallets. Most of the solutions found today build upon smartphone apps. However, wallets, also called agents in an enterprise context, are in development for more professional applications, letting companies use SSI appropriately (Preukschat, 2021).

To allow parties to identify each other within the SSI ecosystem, they use *DIDs*. DIDs are unique identifiers following a standardized scheme. However, in contrast to universally unique identifiers, DIDs are resolvable, similar to a URL. This feature allows DIDs to point to a DID Document, either stored publicly or interchanged peer-to-peer. A DID Document shows meta-data about an identifier, including public keys and gateways, to build up a connection to the respective identity controller (Rhie et al., 2021). As such, DIDs build the fundamental building block to establish a secure connection between parties and look up the public keys of VC issuers.

While most of the interaction of SSI is meant to be bilateral, there is information that should be globally accessible. Such information includes DID Documents of VC issuers, revocation registries for VCs, and standardized templates for VCs. Various solutions are currently developed to implement such a *Verifiable Data Registry*, reaching from web services, over data repositories, and distributed ledgers, i.e., blockchains. While a blockchain is technically unnecessary for SSI, it provides an important way of decentralizing the infrastructure of the Verifiable Data Registry (Nauta & Joosten, 2019; Preukschat, 2021), holding the only information that must be publicly accessible in an SSI system.

SSI is based on the perception that identity holders should actively provide all information. As such, SSI does not make use of hashes stored on the blockchain. Instead, many implementations use a *Cryptographic Accumulator*. For building such an Accumulator, the issuing party generates a huge amount of random numbers. Using modular arithmetic, these numbers will be calculated, forming the Accumulator (Camenisch & Lysyanskaya, 2002). Eventually, the Accumulator is written on the blockchain. When a VC gets issued, one of the randomly generated numbers is assigned to that VC. The user can now perform a proof of non-revocation, demonstrating that their number was

Table 1 Literature on blockchain-based identity management systems for e-government

Author	Description	This study
Sullivan and Burger (2017)	The authors present a blockchain-based eID to enable commercial activities. In particular, the study describes the potential of the Bitnation implementation (Bitnation, 2017) in Estonia. The identity management system makes combined use of a blockchain and the interplanetary file system (IPFS)	In our design, identity holders store their data directly on their devices, reducing the complexity of our system
Elisa et al. (2018)	The authors describe a blockchain-based e-government system for the management of eIDs. The system employs public key cryptography to encrypt privacy-sensitive data written directly on the blockchain	Only non-privacy-sensitive data is written on the blockchain in our design, improving GDPR compliance
Gao et al. (2018)	This article describes BlockID, a framework that uses biometric authentication and a blockchain to manage eIDs. The authors describe how trusted computing technology can bind government-issued digital identities to smartphones	Our design does not yet support the binding of identities to devices
Faber et al. (2019)	This study describes the conceptual design and architecture for a blockchain-based IdM system that primarily focuses on GDPR compliance. The authors propose to use hash pointers pointing to track the registration and validity of identities	Instead of using hash-pointers to track the validity of identities, our design uses privacy-preserving accumulators
Marina et al. (2020)	The authors present an identity system that makes use of blockchain, smart contracts, and IPFS to manage university diplomas. The system has been prototypically implemented using the Ropsten Ethereum test network and an HTML user interface	The use of Hyperledger Indy in our design avoids using smart contracts and the IPFS, reducing the system's complexity
Páez et al. (2020)	This study describes an architecture for a blockchain-based eID system. The system combines smart cards and biometric features for user authentication. The authors propose to use a private blockchain to record and verify all transactions made by citizens	A public blockchain is used for our design, providing easier onboarding of additional members

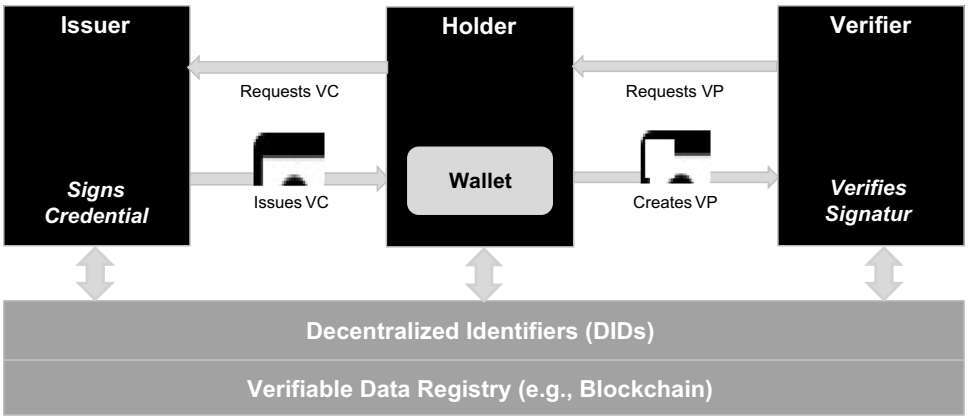

Fig. 1 Fundamental SSI components, based on Preukschat (2021)

Table 2 Overview of the involved experts

ID	Professional title	Field of expertise	Type of organization	Years of experience
IP1	Blockchain Consultant and Researcher	Blockchain Technology	Research Institute	< 5 years
IP2	Blockchain Consultant and Researcher	Blockchain Technology	Research Institute	< 5 years
IP3	Senior Consultant and Researcher	Blockchain Technology	Research Institute	> 15 years
IP4	GDPR and Tax Law Researcher	Legal Tech and Tax Law	Research Institute	< 5 years
IP5	IT Manager	Enterprise IT Projects	IT Service Provider	> 10 years
IP6	Senior Programmer	Enterprise IT Architectures	IT Service Provider	> 15 years
IP7	Consultant	Tax Inspection	Tax Authority	< 5 years
IP8	Business Unit Manager	Tax Inspection	Tax Authority	> 15 years

used to generate the Accumulator. Accordingly, if a VC needs to be revoked, the issuing party can deduct the respective number from the Accumulator, and proof of non-revocation is not possible anymore (Nauta & Joosten, 2019).

Literature on SSI is scarce and either focuses on its potential (Der et al., 2017; Wang & Filippi, 2020) or its technical components (Ferdous et al., 2019; Mühle et al., 2018; van Bokkem et al., 2019). The way such systems should be designed and how they can effectively support business processes is mostly unexplored. Especially its implication for the e-government sector is currently missing.

Method

We followed the DSR paradigm (Gregor & Hevner, 2013; March & Smith, 1995; March & Storey, 2008; Nunamaker et al., 1990) to guide the research project and eventually design the artifact (March & Smith, 1995). In general, DSR aims to contribute to both practice and science. First, DSR aims to solve a practical problem by developing effective artifacts. Consequently, DSR is a natural fit for us as we aim to improve online retailers' tax registration verification process by introducing SSI-based applications. Second, a rigorous research process and an appropriate level of abstraction should help produce design theory as a result of DSR. Depending on the maturity of the artifact, such a theory can be a (medium and grand) design theory, a construct, a method, or a (software) instantiation. With this study, we demonstrate a solution design built on SSI, a software instantiation, and propose four nascent design principles that contribute to the design theory of SSI.

In summary, we chose to employ DSR as it allows us to design an innovative solution to solve a problem with practical relevance. Furthermore, following DSR, we seek to expand the body of knowledge on designing SSI systems, as existing literature lacks in-depth knowledge in this area. In particular, research on real-world applications is missing (Wang & Filippi, 2020). Therefore, the findings from this study should help in making better decisions in designing future SSI-based IdM solutions.

Our study was contextually embedded within a research project initiated by the Bavarian tax authority, which lasted between February 2020 and August 2020. The project primarily served to gain experience with blockchain technology to increase efficiency in tax administration and e-government services. In this way, we were able to draw on eight experts (see Table 2 for more details), whom we involved in defining the objectives for the design solution and evaluating the artifact.

For the development of our design, we followed the approach of Peffers et al. (2007), consisting of the steps

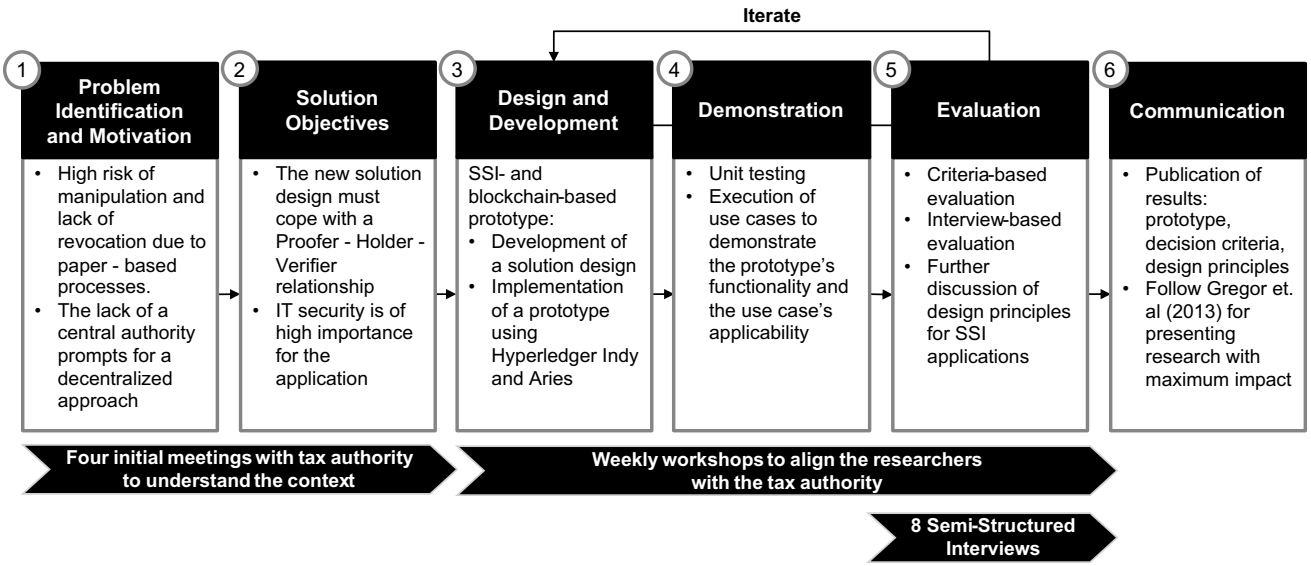

Fig. 2 Design science research process, based on Peffers et al. (2007)

(1) problem identification and motivation, (2) definition of solution objectives, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication. During the research, steps (3) to (5) were conducted highly iteratively (see Fig. 2). Table 3 presents further details on the supporting activities during the research process.

We structured the research project as follows: First, we conducted four initial meetings with the Bavarian tax authority. The meetings took between two and four hours and focused mainly on the processes and legal aspects of the existing approach. The Bavarian tax authority is one of the governing bodies in Germany responsible for issuing proofs of tax registration for online retailers, thus allowing us to better understand the existing solution and identify related problems. We took meeting notes during all workshops. Second, based on these problems, we derived solution objectives to guide our development process. Third, we applied the concept of SSI to the problem area and designed an innovative solution. To demonstrate the applicability and effectiveness of the artifact, an IT service provider eventually implemented a prototype. In weekly meetings, the prototype was continuously presented and discussed with consultants, managers, and potential system users at the tax authority. This approach allowed us to test the design continuously and provided ongoing guidance for further improvements. Once we perceived a sufficient level of maturity, we went over to the final evaluation of our design. To evaluate the developed artifact, we employ a mixed-methods approach. In particular, we used literature and insights from the artifact's development to assess whether the artifact meets the predefined design objectives. To gain additional insights, we also conducted eight interviews. Prior to the interviews, each interview partner could extensively use the developed prototype, including the issuance and verification of VCs. The interviews took between 45 and 60 min. We started with general questions about the interviewee and later inquired about discussing whether the artifact meets their requirements and, in case there were still problems, what needs to be improved. To analyze the interviews, we used qualitative techniques, including transcribing and coding the interviews (Mayring, 2014). Finally, abstracting from the case-specific design, we used our insights to formulate four nascent design principles for SSI systems.

Problem identification

The growing dissemination of Internet marketplaces poses a significant challenge to tax authorities. Retailers offer their goods in Germany but may not meet their tax obligations, which results in considerable tax losses. The German legislator has reacted to this situation by introducing recording obligations for operators of electronic marketplaces. Marketplace operators will be required to obtain a tax registration certificate from their retailers. Retailers must apply for this certificate at their responsible tax office. At present, the application and issuance of the certificate are conducted in paper form. Figure 3 describes the current process as a business process diagram[1].

[1] We adhered to the BPMN v2.0 specification as outlined on https://www.bpmn.org/

Table 3 Supporting activities during the research process

Activity	Description	Participating experts	Used data and artifacts	Outcome
Initial meetings	Initial meetings with the tax authority focused on understanding the processes and legal aspects to identify related problems	IP1-IP4, IP7-IP8	- Legal definitions and opinions concerning the given case - Internal reports covering the paper-based processes	- Description of the paper-based solution - Problem definition of the paper-based solution - Design objectives for an improved solution
Weekly workshops	Weekly workshops to continuously present and discuss the progress of the prototype development and make improvements based on the given feedback	IP1-IP2, IP5-IP7	- Data models (e.g., for VCs) - Mockups and prototypes of user interfaces - Process models - System architecture diagrams	- Intermediate evaluation of the SSI design - Feedback from experts regarding further improvement possibilities for the next design iteration
Interviews	Eight interviews to gain additional in-depth insights regarding the effectiveness of the final artifact	IP1-IP8	- Fully functional prototype of the SSI system to support the verification of online retailers	- Final evaluation of the SSI artifact - Description of the effectiveness of the artifact, including its strengths and weaknesses

Manual activities characterize the entire process flow, leading to high expenses, especially concerning marketplaces since they must manually check the respective paper certificates. Besides, the document's authenticity is difficult to verify as no further measures exist to protect the document against forgery apart from the tax authority's official stamp and signature. Thus, certificates might be manipulated without significant hurdles in the paper-based process. Finally, the most significant drawback is that it is not possible to revoke the certificate. The tax registration also expires when a retailer unsubscribes from its tax office. This fact should consequently also affect the certificate. While the current solution would allow the tax authority to collect the issued paper certificates, this procedure is still impracticable as scans allow for further use of copies.

Design objectives

We aim to develop an improved solution that should support the particularities depicted in Fig. 4 The retailer must identify themselves to apply for a tax certificate. After the application, the respective tax authority issues a certificate with all the required characteristics. The retailer can then use this certificate to prove they are properly registered with the tax authority. The marketplace must be able to verify the information given by the retailer. It should no longer be possible to provide evidence of the tax registration if the taxpayer or market participant no longer meets the requirements. In this case, it should be possible to set the certificate's status to "invalid".

We used workshops with two employees of the tax authority along with literature to derive eight design objectives (see Table 4).

Design and development

We started our design phase by discussing centralized solutions. However, a missing central authority and a high number of stakeholders led to the final solution design based on SSI, using blockchain as a Verifiable Data Registry. At first glance, using a blockchain in public administered use cases might look inappropriate, as typically, there should be no trust issues arising. However, political and legal barriers often prevent the centralization of competencies in many western countries, which makes blockchain a potential alternative. Rieger et al. (2019) provide detailed insights into the applicability of blockchain for the public sectors, especially within Europe. Thus, data protection of blockchain (in combination with modern cryptography) and promises regarding interoperability have strengthened our decision for blockchain and an SSI approach. Figure 5 depicts our study's final

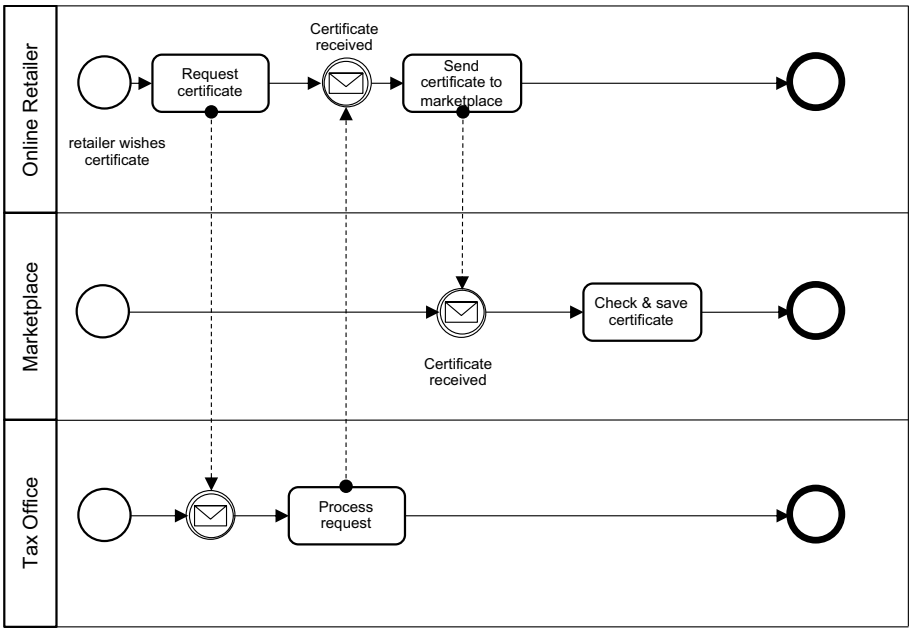

Fig. 3 Description of the current paper-based process

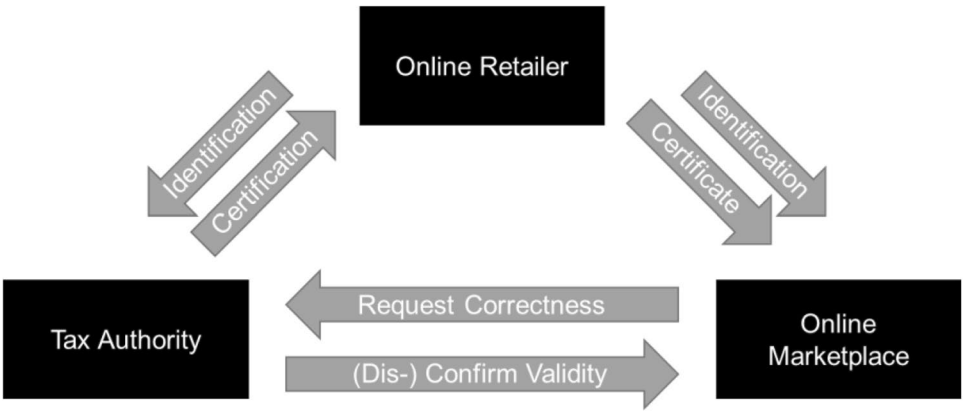

Fig. 4 Simplified overview of the process

design, incorporating the SSI building blocks and legacy database systems. While the tax authority is responsible for providing certification of tax registration, the citizens' office issues an identity VC for the online retailer.

The system comprises five distinct process steps: preparation and initial setup, onboarding via an identity VC, issuance of the tax VC, presentation towards the marketplace, and revocation. We explain each step in more detail in the following.

Initial system setup

While SSI makes heavy use of peer-to-peer exchange of VCs, a Verifiable Data Registry has to be set up first. We decided on Hyperledger Indy as a permissioned public blockchain for the given case. This decision contrasts with other architectures for e-government solutions, such as Rieger et al. (2019) or Yavuz et al. (2018), who typically propose private permissioned or public permissionless blockchains. We differ from previous literature due to the following reasons. First, we wanted to ensure high reliability and level of assurance regarding the data provided by the system. The blockchain acts as a single point of truth, mainly for the decentralized PKI. Thus, parties must trust its data. This requirement calls for tight control over who can write data to the blockchain and use it to issue VCs later. Therefore, we opted for a permissioned system. Second, while we wanted to restrict who can write on the blockchain, potentially, any party should be able to query data written on the blockchain as its data is needed to verify the validity of VCs. This requirement led to the use of public accessible blockchain infrastructure.

We used the BCovrin Test network as a concrete implementation of Hyperledger Indy as infrastructure for our prototype.[2] In the future, a (partly) state-owned blockchain

[2] http://test.bcovrin.vonx.io/

Table 4 Design objectives for the SSI system

Design objective	Description	Reasoning	Evaluation
Issuance	The system should allow the issuance of 1) a certificate to prove the retailer's identity and 2) a certificate to prove that the retailer is correctly registered at the tax authority	According to German law, documents certifying tax registration shall be issued	Evaluation of fulfillment
Verification	The system should facilitate the tax authority and the marketplace to verify certificates. For verification, it is necessary to check the validity, signature, and integrity of the certificate	The existing paper documents had only rudimentary protection against forgery. The tax authority wished for greater protection against modification	Evaluation of fulfillment
Revocation	Suppose the underlying information of a certificate has expired, e.g., the retailer's address or status changes. In that case, the system must allow the issuing party to mark the certificate as invalid. The revocation should ensure that the verifier knows that the certificate is not valid anymore	The existing paper documents had a temporal validity since it was easy to copy and, thus, a retraction of the physical copies was therefore not meaningful. However, the tax authority wanted the option to deactivate documents without delay and at relative ease	Evaluation of fulfillment
Audit	The tax authority should be able to audit the verification process of the online marketplace. Thus, it should be possible for the tax authority to confirm that the marketplace complies with the law and requests and verifies the tax registration of its retailers	From the point of view of the tax authority, the use of a paper document was highly opaque. With a new IT solution, the tax authority assessed the option that the audit of regulatory compliance of the retailers would be made easier	Evaluation of fulfillment
Decentralization	No central authority should oversee all documents and attributes, thus requiring a decentralized and interoperable IdM approach	In Germany, data holdings between individual agencies are highly fragmented. This is required by law to avoid merging and thus a glassy citizen. However, the tax authority still wanted a system that worked across authorities and private organizations to foster seamless interoperability	Evaluation of independence from other organizations
Data confidentiality	Confidentiality defines the property of data or information intended only for specific recipients. Confidentiality can be promoted or enforced by technical means (Whitman & Mattord, 2011). It must be ensured that data about individual parties is only accessible to them and the parties directly involved in the process	In Germany, the privacy of tax information is subject not only to the GDPR but also to tax secrecy. During the workshops, all tax authority employees mentioned that data protection was one of the essential requirements. This requirement should be prioritized before all other requirements	Evaluation of data disclosure
Data availability	Availability describes the probability that a system can provide the service at a certain point in time. Its reliability, maintainability, and redundancy typically measure a system's availability (Whitman & Mattord, 2011). The system should ensure constant availability	Since many online retailers and marketplaces are directly dependent on the use of the system, a high level of availability is required in order not to jeopardize the business processes of all parties involved	Evaluation of the availability of infrastructure
Usability	The usability dimension describes how easily and intuitively the end-user can use the system. Complex graphical user interfaces and processes can lead to strong user dissatisfaction and negatively influence use (Byun & Finnie, 2011). The application and handling of a certificate should be designed as intuitively as possible concerning the present use case	Even if the system fulfills all technical requirements, high hurdles during use can lead to serious problems. Since both very large and small retailers need to use the system, the respective barriers must be kept low	Evaluation of required interactions

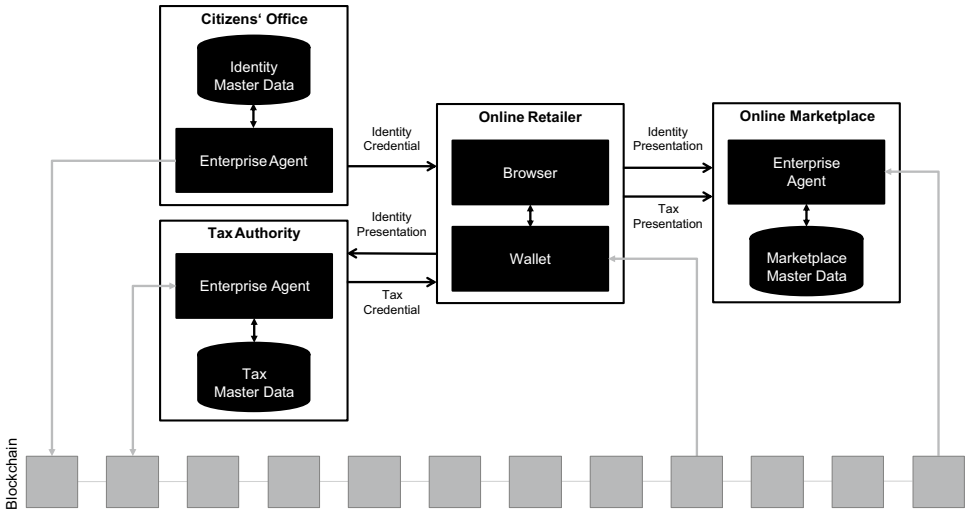

Fig. 5 SSI-based tax verification system

```
"did_document": {
        "id": <citizens' office DID>,
        "assertionMethod": [
                {
                    "id": <key-id>,
                    "type": "CLSignature2019",
                    "controller": <citizens' office DID>,
                    "publicKey": <public Key>,
                }
        ]
        "service": [{
                "id": <service ID>,
                "type": "LinkedDomains",
                "serviceEndpoint": "https://citizen-office.eu"
  }]
}
```

Fig. 6 Citizens' office DID Document

might be desirable, where the citizens' office and the tax authority run their peers. Alternatively, projects such as European Blockchain Service Infrastructure even suggest that pan-European, cross-state operations would be possible in the future (Williams, 2020). Regardless of the physical nature of the blockchain system, both the citizens' office and the tax authority have to be entitled as endorsers to publish relevant information. Once the authorities are registered as endorsers, they can publish their DID Documents, including their public DID (see Fig. 6 for exemplary JSON of the citizens' office DID document), their Credential Definitions, and the respective Accumulator (see Fig. 7 for exemplary JSON of the identity VC definition) on the blockchain.

The DID Document contains all relevant information of a certain issuer that is required to establish a secure connection to it and, second, to later verify the signature of the VC. Therefore, the DID Document published on the blockchain consist of the keys used by the authority, the respective cryptographic algorithms, and the service gateways through which the authorities can be reached (Preukschat, 2021). The citizens' office and the tax authority write a DID Document on the blockchain. To later provide this information, a party can use the DID of the respective authority to resolve the related DID Document.

Next, the authorities can create a Credential Definition and write it on the blockchain. The Credential Definition holds all meta-data for a VC. This data includes the mandatory data fields of a VC, the revocation method, if applicable, and the DIDs of the authorities acting as the controller of that definition. We would like to note that similar to the DIDs that can be used to resolve a DID Document, Credential Definitions also have identifiers that can later be

Fig. 7 Identity VC Credential Definition

```
"credential_definition": {
        "version": "1.0",
        "id": <credential-id>,
        "tag": “base credential”,
        "controller": <citizens’ office DID>,
        "type": "CLSignature2019",
        "attrNames": [
            "companyName",
            "companyAddressCountry",
            "companyAddressLocality",
            "companyAddressRegion",
            "companyPostOfficeBoxNumber",
            "companyPostalCode",
            "companyStreetAddress",
        ],
        "revocation": {
            <accumulator>
        }
}
```

used to resolve the Credential Definition. The verifier can, thus, include this Credential Definition identifier to ensure that it can only be answered with VCs that follow this exact Credential Definition. With the creation of the Credential Definition, also an Accumulator is written on the blockchain. The Credential Definition points to this Accumulator and allows parties to access the Credential Definition to resolve the Accumulator. In turn, the Accumulator represents the revocation registry of the respective VCs (Camenisch & Lysyanskaya, 2002; Nauta & Joosten, 2019).

Lastly, online websites were developed to facilitate the connection of the online retailer's wallet with the respective enterprise wallets. We used HTML, Javascript, and Trinsic Agents with Trinsic Studio[3] to implement the web services and the enterprise agents. Figure 8 depicts one of the developed web interfaces used to set up a secure connection to an enterprise agent by scanning the QR code with the smartphone wallet. If a desktop wallet should be used, the online retailer might open a link instead of using the QR code.

[3] https://trinsic.id/trinsic-studio/

Onboarding the online retailer

In the first step, the IdM system has to onboard the online retailer. This procedure aims to provide a VC representing the retailer's master identity that they can use for different processes within the system. Similar to the German citizen identity, the citizens' office will issue the respective VC (see Fig. 9).

First, the online retailer applies (1) for their first VC at the citizens' office's website. As this VC does not yet represent their tax registration but rather the master identity data, we name it identity VC. To identify themselves, they might use their identity card and video ident. Once applied, an invitation link is generated by the responsible citizens' office's agent (2). The link will be provided in the form of a QR code, which allows it to be sent via paper to the retailer or online via a website or e-mail. The online retailer can open this link using their SSI wallet by scanning the QR code. The link establishes a secure connection between the retailer's wallet and the citizens' office's SSI agent (3). This process step also includes the exchange of the DID Documents between the online retailer and the citizens' office. All

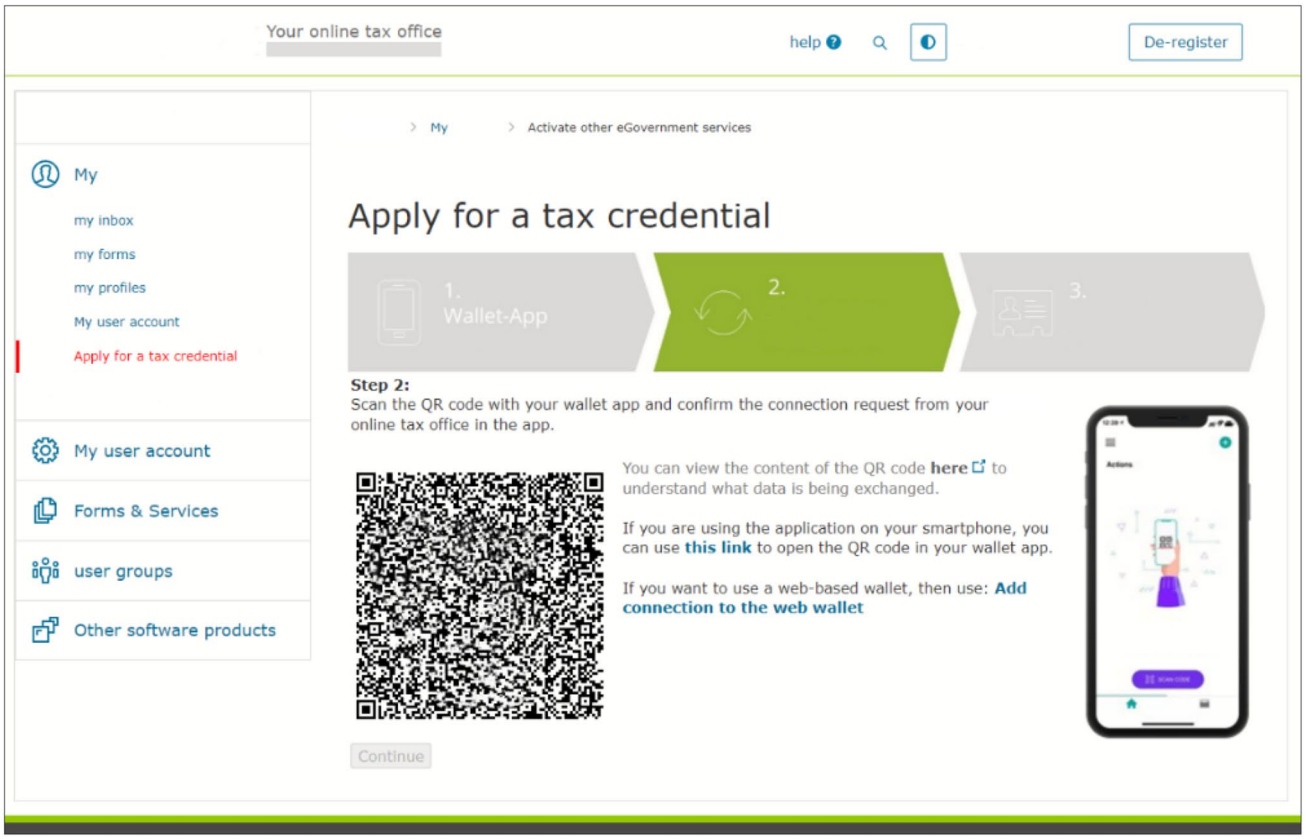

Fig. 8 Online web interface of the tax authority

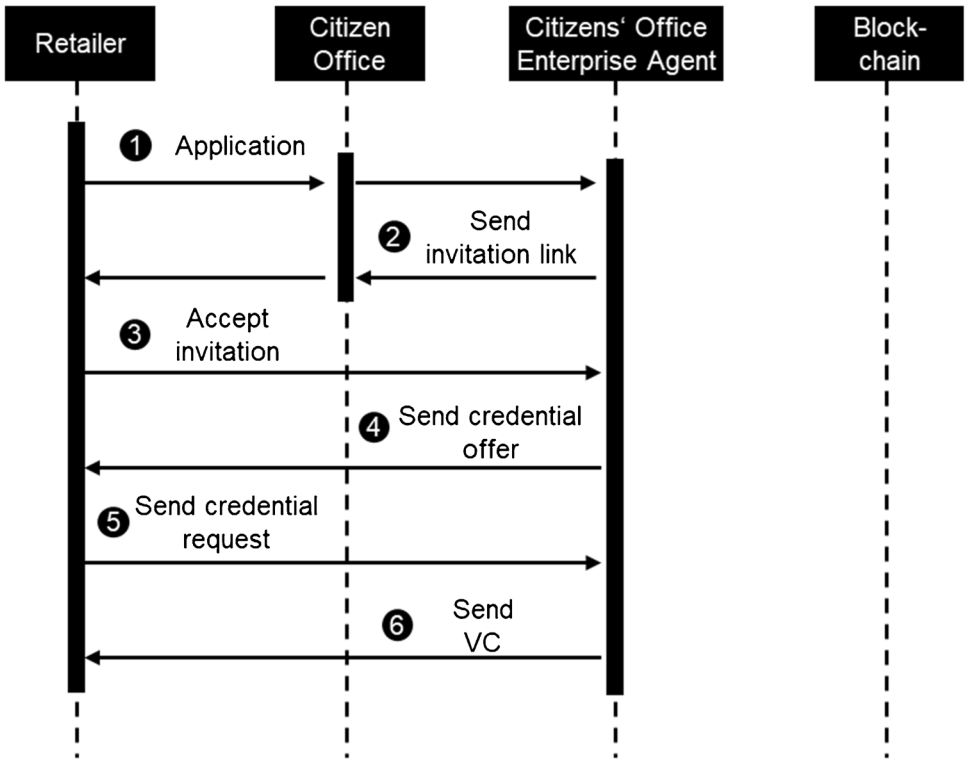

Fig. 9 Issuance of the identity VC

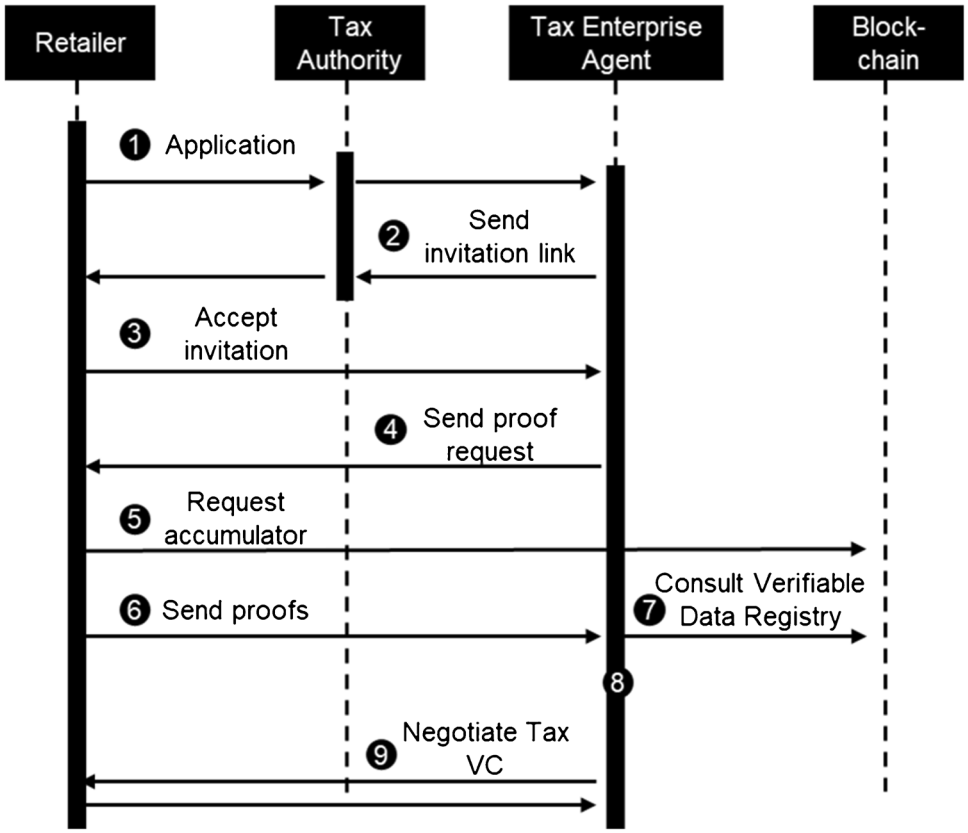

Fig. 10 Issuance of the tax VC

communication now runs over a secure and direct connection between the retailer's wallet and the citizens' office's agent. Next, the citizens' office's agent sends a credential offer to the online retailer's wallet (4). If the online retailer accepts the VC in the proposed form, it sends back a credential request (5). The citizens' office's SSI wallet finally sends the corresponding VC back to the online retailer (6). No transaction on the blockchain is required yet for the VC's issuance. The revocation works similarly to a blocklist, meaning that all VCs are valid by default. We consider this an effective design decision because there was no need to issue invalid VCs, which allowed us to drastically reduce the number of transactions written to the blockchain. As the VCs are cryptographically signed, there is also no need to store the hash of the certificate upfront, unlike what has been suggested by other researchers (Haddouti & Ech-Cherif El Kettani, 2019).

Issuance of the tax verifiable credential

To confirm the tax registration, the tax authority will issue the tax VC to the retailer, representing the tax registration (see Fig. 10). For the second VC, the online retailer applies for the appropriate credential via the web portal of the tax authority. Steps (2) and (3) are analogous to issuing the identity VC and establishes a secure connection between the retailer's wallet and the tax authority's agent. The tax authority's agent now expects the online retailer to prove the master data, such as name and address, from their identity VC (4). The online retailer retrieves the latest Accumulator status from the blockchain (5). With this data, the retailer creates proof of identity, including proof that the underlying identity VC is not revoked, and sends the VP to the tax authority's agent (6). The tax authority's agent now queries the Accumulator value of the identity VC and the DID Document of the citizens' office from the Verifiable Data Registry (7). Both are used to verify the validity and signature of the VP. The tax authority then internally checks the proof's contents and whether the proof of identity matches the identity for the requested tax registration (8). Suppose the online retailer could authenticate themself with their identity VC. In that case, the tax VC is issued using the same procedure as the issuance of the identity VC at the citizens' office (9). The online retailer finally stores the tax VC in their wallet. Only read requests from the blockchain are required to obtain the current Accumulator, and again no write transactions are needed.

Proof of identity and tax registration

The retailer can now use both VCs to prove the underlying attributes (see Fig. 11). To do so, the online retailer first logs

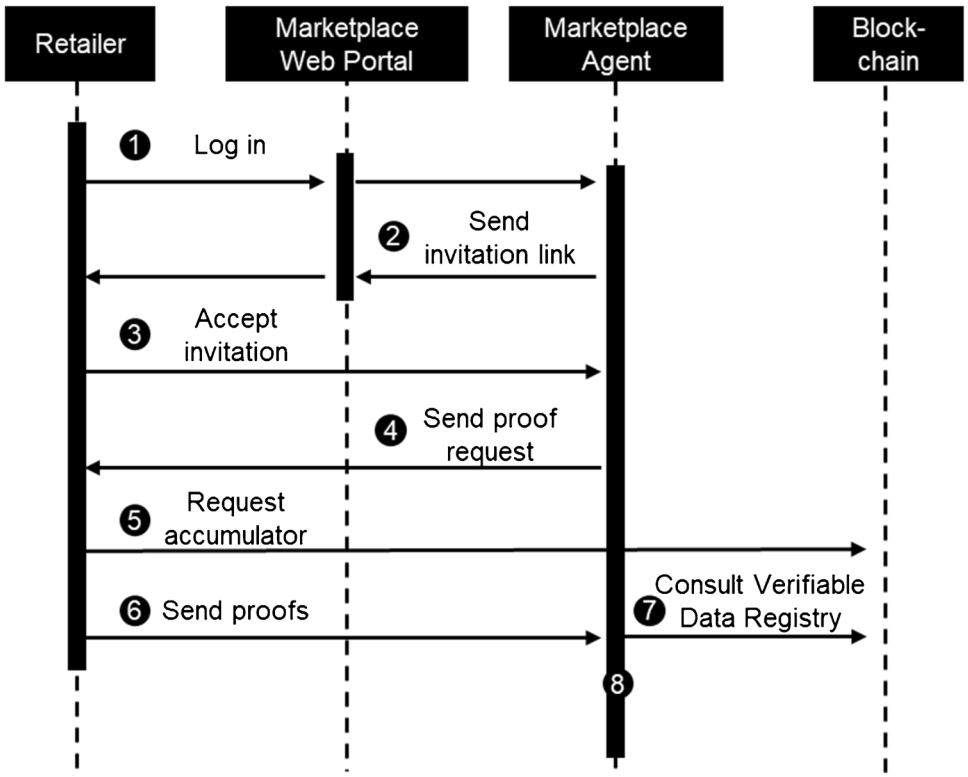

Fig. 11 Presentation toward the marketplace

themself into their account on the marketplace's web portal (1). Again, a secure connection is established by exchanging an invitation link and the DID Documents via (2) and (3). In the next step, the marketplace creates a proof request and sends it to the online retailer (5). The proof request contains a detailed list of the required attributes and who should certify these attributes. In the given case, the attributes must provide general identity information, proof of tax registration, and evidence that the citizens' office and tax authority have issued the underlying VCs. Upon receiving the proof request, the online retailer processes the corresponding request, including retrieving the latest Accumulator value (6). The process is very similar to the presentation towards the tax authority. However, the retailer's wallet now combines attributes from the two previously obtained VCs, i.e., the identity VC and the tax VC, into a single VP and sends it to the marketplace (7). The marketplace can now use the Verifiable Data Registry (i.e., the blockchain) to retrieve the DID Documents from the citizens' office and the tax authority (including their public keys and signing method) as well as the Accumulator status of the VCs (8). Then the marketplace can use cryptographic methods to validate the proofs and confirm the online retailer's identity and the validity of the tax registration (9).

Revocation of a verifiable credential

It can happen in individual cases that tax registrations of individual retailers might no longer be valid or that an identity VC needs to be revoked due to changes in the retailer's corporate information, such as the company address or discontinuance of business. This situation requires the possibility of marking individual VCs as invalid. For this purpose, the tax authority or the citizens' office can adjust the data stored on the blockchain so that the factor representing the validity of the VC now returns "invalid". From this moment on, the retailer can no longer create valid proof of non-revocation. If necessary, a VC with the new data can then be issued. The possibility of revocation also leads us not to integrate master identity data in the tax VC. As such, attributes can be revoked independently from each other, and no dependencies exist.

Demonstration and evaluation

An IT service provider prototypically implemented the proposed design with Hyperledger Indy (Hyperledger Indy, 2020) and Aries (Hyperledger Aries, 2020) at the Bavarian tax authority. We used these frameworks as they follow the W3C standards and have a growing community. The implementation includes all central components of the design, enterprise agents, graphical user interfaces, and the blockchain environment. Furthermore, we employed the Trinsic Wallet available on the Android and Apple App Markets. As a public blockchain, we used the BCovrin Test Network to allow for easier integration of different stakeholders. The

prototype permitted us to evaluate the system beyond a conceptual level. We involved managers and potential users in workshops and presentations to demonstrate the prototype, checking whether it meets their expectations. In particular, the prototype allowed users to play along with the entire process, starting from the issuance of the first VC until the presentation of the tax registration.

The general feedback from the experts was positive. The interviewees largely approved that the system addresses the current problems. They especially highlighted that the system provides very good integrity and privacy characteristics. IP3 says that these traits are especially important in governmental applications, where citizens must rely on respective information. With this, IP4 positively noted the use of an Accumulator to store the validity of credentials and said: "that if hashes were used, it would be much more difficult to implement [such a blockchain-based system] from a data protection point of view."

Asking about differences to a hypothetical centralized approach, IP1 stresses that the availability of the blockchain is an essential benefit. In the presented case, any downtime must be avoided since this could lead to retailers no longer being able to prove their registration. "A marketplace could even run its own node" (IP1), allowing a high level of redundancy. IP2 furthermore added that the decentralized infrastructure also allows "to shift the responsibility away (…) from the tax authority [to the marketplaces]". As such, marketplaces can be involved in the accountability for the availability of the system. Finally, also addressing the comparison to centralized systems, IP5 said "that an individual solution would probably not bring as much benefit as a generic solution". The interviewee emphasized that SSI could provide an "open and generic" platform for many future applications. For the given case, IP5 actually only sees marginal benefits of SSI over a conventional PKI. However, having the option to further expand the system in any direction with very flexible governance "is the real benefit compared to a normal PKI".

We also inquired with the experts about the differences between the SSI system in comparison to other blockchain-based IdM systems. One of the most dominant answers from the interviewees was that the ecosystem built around SSI is to be considered a major advantage. IP5 states that "many solutions are based on the same technology and the same standards", which is "the key that gives SSI the greatest potential" (IP5). Similarly, IP1 points out that other blockchain solutions are often proprietary or do not follow any standards, lacking common technical specifications as an important requirement for interoperability. As such, the expert positively remarked that we follow the W3C standards for DIDs and VCs and employ Hyperledger Aries and Indy as development frameworks. Accordingly, another expert expects that different SSI applications currently under development will be interoperable on a technological level due to these specifications (IP8). Nevertheless, the employed solution still requires all parties to be on the same blockchain, as cross-blockchain implementations of VCs are still in development in the given frameworks (IP6). As such, IP6 points out that "it is essential that the interoperability between different blockchains has to improve", so that full portability can be established.

The interviewees also point out one major issue of the system. IP7 commented that it would be easier to just let the marketplace monitor the tax registration status. With SSI, the retailer must always arrange for the creation of a VP proving that he is still registered: "Now if you imagine a retailer who is constantly selling something [on different marketplaces], then it is difficult to implement a process if there always has to be an impulse from the retailer for every marketplace" (IP7). Even though IP8 generally agrees that the SSI application requires additional efforts, he still thinks that it is a better solution than giving marketplaces direct access to revocation information: "Of course, this would be a security risk, as access tokens might be stolen and then used by others" (IP8).

Table 5 shows the consolidated results of our evaluation with regard to the predefined design objectives. In general, the developed IdM system satisfies the functional requirements. It provides means for the issuance of credentials, derivation of proofs, and verification of proofs. Besides, all aspects of IT security showed very good results. While the blockchain ensures the availability of organization-spanning features (i.e., the validity registry), cryptographic signatures and proofs allow for integrity and privacy. However, especially features for auditing and usability still show further room for improvement.

Discussion

Our evaluation shows that SSI can provide a solid infrastructure for a decentralized, cross-organizational IdM system. While organizations retain their legacy databases and systems, SSI provides an overarching identity layer to transfer identity information across different organizations, which would otherwise be characterized as data silos.

Description of the SSI artifacts

From an infrastructure perspective, two components are essential for the SSI system to function (see Table 6). First, Wallets and Agents provide a means of handling VCs, VPs, and connections between parties. Thus, they provide the main way of bilateral communication between a holder and the issuer or the verifier. We heavily discussed with the practitioners whether a custom wallet would bring benefits

Table 5 Evaluation of the artifact

Design objective	Evaluation
Issuance of certificate	SSI potentially allows any party to issue VCs (Mühle et al., 2018). The citizens' office can use this property to issue a VC to the retailer that provides their master identity data in the given context. Furthermore, the tax authority can issue a VC that allows the retailer to eventually prove their tax registration. This approach mimics a digitized procedure of the existing paper-based process
Verification	Before the issuance, all VCs will be signed by the issuing party (Mühle et al., 2018). The retailer can then use the issued VCs to create VPs and demonstrate them to the verifying party. Based on a VP, the verifier can verify the authenticity of the underlying VC, including that it has not been altered and the issuer's signature (Preukschat, 2021). In contrast to the paper-based approach, the interviewees agreed that protection against manipulation had been significantly improved. IP7 states that "in terms of anti-counterfeiting, [SSI] is definitely better. So compared to the paper solution, it's better"
Revocation	Using the blockchain and its Accumulator (Mühle et al., 2018), the citizens' office and the tax authority can mark their issued certificates as invalid. This results in the effect that the retailer is no longer able to provide proof of non-revocation. Nevertheless, the marketplace receives no notification about the invalidity of the tax registration. As such, we consulted with IP7 and IP8 and decided to require the retailer to perform periodic proof of non-revocation every 14 days, balancing out costs and legal certainty. Even with this limitation, the employees of the tax authority agreed that the SSI system offers a significant advantage over the existing paper-based approach, which does not allow revocation in the first place (IP7, IP8). IP7 discusses that "the revisability of certificates or validity (…) is one of the arguments in favor of SSI. And we wanted to have that for the implementation of this case, something you cannot do with paper certificates"
Audit	SSI focuses on providing a high level of privacy. Thus, most processes are only bilateral and do not engage the blockchain (Mühle et al., 2018). Furthermore, the employed frameworks, namely Hyperledger Indy and Aries, do not provide means for a third party to review any processes. Thus, the tax authority cannot audit the compliance of the online marketplace and its retailers. However, the paper-based process also had this limitation, as the activities were not visible to the tax authority here either. IP2, however, finds that this might even be an advantage for SSI solutions: "This is also an advantage for privacy because third parties can no longer log processes, precisely because the data exchange happens bilaterally " (IP2)
Decentral-ization	Blockchain provides a decentralized and interoperable infrastructure for all involved parties (Ferdous et al., 2019). Instead of storing revocation data on a centralized server of a certificate authority, issuers can use the blockchain as a Verifiable Data Registry to provide the information (Wang & Filippi, 2020). IP5 stated that for him, decentralization was one of the main reasons to use SSI: "But this decentralized approach, (…) that really excited me from the beginning, I have to say " (IP5)
Data confidentiality	Except for the Accumulator and public DIDs stored on the blockchain, all relevant data is only available to the process's respective participants. In general, most processes are bilateral and promote data confidentiality by design (van Bokkem et al., 2019). For example, the issuance of a VC only involves the issuer and the holder or the holder without engaging third parties or intermediaries. IP4 summarizes: "This means that personal data is not actually included in the blockchain. And everything that is relevant to data protection lies directly with the data owner" (IP4). In this respect, SSI is no different from the paper-based procedure, in which data relevant to data protection also reside only with the owner
Data availability	As a decentralized system, the blockchain inherently has high reliability, and revocation information will be consistently available: "Of course, the operation of many peers [of a blockchain] also means greater effort. But you can be sure that at least one of them is always available" (IP1). All other components are solely hosted at the sides of the respective parties. Therefore, they must rely on conventional mechanisms, such as replicants, to provide data availability (Faber et al., 2019)
Usability	The processes of the system are similar to the analog processes of the existing solution. Instead of a paper document, a digitally signed file is now transferred to the holder. The holder can then present the underlying properties using his/her smartphone. However, the proposed design still requires many interactions, including scanning several QR codes and accepting various requests. As such, usability in the enterprise context still offers room for improvement. IP8 even points out that the usability of the prototype is not feasible for productive operation: "But in terms of handling, it is, of course, impossible for [companies] to do it that way. They can't always scan something with their phone" (IP8)

over existing offerings readily available on the market during the project. The discussion was also driven by whether a public authority should provide their own wallet to the citizens, also allowing for branding it as an official wallet developed by the authorities. Finally, we refrained from the idea, mainly due to the high expenses of developing a secure wallet from scratch. Rather, during the evaluation phase, we tested a wide variety of mobile apps and demonstrated the compatibility of the developed system with these apps. As such, citizens will be able to choose the app they like without any niceties to use a state-developed application, as long as these apps follow the W3C DID (W3C, 2021a) and W3C VC (W3C, 2021b) standards. Nevertheless, wallets provided by the authorities might still be viable in the

Table 6 Description of used infrastructure and SSI artifacts

Infrastructure	SSI artifact	Case-specific use	General use
Verifiable Data Registry (Public, multilateral)	Public DID and DID Document	The citizens' office and tax authority issue a public DID that resolves to a DID Document on the blockchain so that the marketplace can verify credentials issued by them. The DID Document includes their endpoints, public keys, and used cryptography	Public DIDs allow issuers to point to publicly available information (i.e., DID Document) so that third parties can verify the digital signatures on the respective credentials. That approach is useful for cases with a prior unknowable number of parties and where privacy is no issue
	Revocation Accumulator	The tax authority uses an Accumulator written on the blockchain to enforce revocation. For example, if an online retailer is no longer registered, the tax authority can revoke the respective VC	The issuer maintains a revocation Accumulator for each issued VC type. VC holders can use the revocation Accumulator to prove that a VC is still valid
	Credential Definition	The tax authority and the citizens' office create a Credential Definition that specifies what the proof of master data and tax registration should look like. The online marketplace can specify these Credential Definitions with the proof request to ensure that the VP roots in the VCs issued by the tax authority and the citizens' office	Credential Definitions allow issues to specify the content and general properties, such as signature type and revocation Accumulator for their credentials. Verifiers can include the ID of the Credential Definition in their proof request, which specifies the root of proving for the VP
Wallet/ Agent (Private, bilateral)	Private DID and DID Document	The online retailer and the online marketplace use private DIDs to establish communication with other parties. The respective DID Document is exchanged only peer-to-peer and is not published	Private DIDs allow establishing a secure connection between parties without the need to publish them on the blockchain. They are used for pairwise communication and when privacy is a relevant factor
	Verifiable Credential	The citizens' office and the tax authority issue cryptographically signed Verifiable Credentials to certify the master data and the tax registration of the online retailer	Verifiable Credentials allow claims made by a particular party to be verifiably certified using tamper-proof cryptographic measures
	Verifiable Presentation	Based on their verifiable credential, the online retailer creates a Verifiable Presentation to prove identity towards the tax authority and identity as well as tax registration towards the online market. Thanks to Verifiable Presentations, the identity VC and the tax VC remain only in the wallet of the online retailer	VPs allow deriving traceable claims from VCs. Thus, the VC remains with the identity holder, preventing third parties from using the underlying VCs

future, for example, to allow for eIDAS compliance and a higher level of assurance.

Second, the Verifiable Data Registry provides a publicly available infrastructure. An SSI system stores public DIDs, respective DID Documents, revocation lists, and Credential Definitions in the Verifiable Data Registry. Currently, most SSI frameworks use blockchain for the Verifiable Data Registry (Preukschat, 2021). Nevertheless, during the development, we also discussed centralized ways of implementing the Verifiable Data Registry, where the tax authority and the citizens' office each would have their own server, managing their respective data. Unfortunately, the Hyperledger Aries framework does not yet implement the option to combine VCs governed by two different Verifiable Data Registries. As a result, there would be two independent SSI systems, failing to provide a common ecosystem. In addition, taking the promises blockchain makes towards sophisticated decentralized governance in e-government applications (Rieger et al., 2019) and IT security, including availability, blockchain still offers some benefits over centralized systems. Nevertheless, once future iterations of SSI frameworks are available, potentially powered by projects such as a Universal Resolver for different registries (Decentralized Identity Foundation, 2021), hybrid-governed SSI ecosystems may potentially arise. In such a hybrid scenario, one SSI ecosystem might be supported by several Verifiable Data Registries. Depending on the use case, such registries might run on central servers, one or more blockchains, or a combination of these options. Research into how such hybrid systems for SSI can look and how they provide benefits offers scope for further research.

Comparison of SSI to alternative solutions

Throughout the research project, we compared the SSI system to other alternatives, i.e., the current paper-based process and the current implementation of eIDAS (see Table 7).

As our evaluation shows, it is evident that the paper-based process shows a wide range of challenges that SSI can address. From a function point of view, the process when using SSI is very similar to using actual paper-based certificates. There is still an issuer who hands out a document to a holder, and the holder still shows the properties of this document to a third party. However, while SSI follows very similar procedures, it allows the entire process to be completely digital. In addition, SSI enables a few more features, for example, the easy revocation of documents. While it is possible to physically collect issued documents in an analog process, it is associated with high costs or even completely impracticable if the document can be copied at will.

Since the study was strongly motivated by the shortcomings of the current eIDAS implementation, we also like to compare it to the presented SSI solution. Several factors

Table 7 Comparison of SSI to alternative solutions

	Paper-based certificates	eIDAS	SSI-based eID
Identity subject	Certificates can cover any subject, including legal entities and natural persons	The eID is only applicable to natural persons	VCs can cover any subject, including legal entities and natural persons
Attributes	Certificates can cover any attributes, including master data and additional properties (via one or multiple certificates)	The eID is restricted only to master data	VCs can cover any attributes, including master data and additional properties (via one or multiple VCs)
Security	Paper-based certificates show a limited level of security. Certain hurdles can be set to prevent the copying of certificates (e.g., stamps and watermarks), but it is not possible to prevent it completely	Digital signatures effectively prevent the possibility of forgery or manipulation of the eID and allow the verification of the issuer. The use of hardware tokens also prevents the duplication of eIDs	Digital signatures effectively prevent the possibility of forgery or manipulation of VCs and allow the verification of the issuer. However, it is still possible to transfer wallets to other devices without authorization
Easiness of integration	No integration is needed	The eIDAS resembles a closed system with a high regulatory burden to enter it	Companies only need access to a common ledger and the corresponding authorizations to use it
Effort for revocation	Revocation is only possible if the certificate is physically collected again. This is associated with high costs or is even completely impracticable if the document can be copied	Revocation is carried out via central revocation registers and therefore involves little effort	The revocation is done by an Accumulator on a common ledger. An adjustment of the Accumulator can be made with appropriately low effort

speak to the advantages of SSI. First, SSI is not limited to private individuals. Currently, identities for legal entities are not provided for in eIDAS. Thus, a merchant who is not a natural person cannot prove his identity (European Commission, 2021). SSI is agnostic in this sense and provides a technical basis for both natural and legal persons. Second, eIDAS does not allow the representation of additional attributes besides the master data (EUR-Lex, 2014). This means that the tax registration information cannot be depicted at all with eIDAS. Again, SSI is potentially more flexible and allows any form of attribute evidence, requiring only a schema to be published in a common ledger. Third, integrating private companies into the eIDAS ecosystem is often seen as too expensive and too burdensome (European Commission, 2021). Here, SSI has the advantage that auditors can easily develop use cases based on SSI, especially when using public blockchains. Nevertheless, it is important to mention that eIDAS still has specific advantages over SSI in terms of security. In particular, SSI does not yet meet the highest requirements regarding level of assurance, especially the option to bind certificates to devices (EUR-Lex, 2014). Currently, there are no hardware tokens, e.g., smart cards, that enforce device binding for SSI. Following the opinion of the interviewees, this is not relevant in the case described in this article, as even a lower level of assurance suffices. However, for very sensitive applications, e.g., in the financial sector, the very high level of assurance that eIDAS implementations can provide might be necessary. Future research should therefore try to incorporate solutions that use trusted computing technology (Gao et al., 2018) with SSI.

Derivation of design principles

While the IdM system development was highly motivated by the use case, the general applicability of the developed system beyond this field was considered throughout the entire project. Therefore, we follow the general conception that SSI systems should be thought out in a broader context facilitating interoperability between different applications and use cases (Mühle et al., 2018; Wang & Filippi, 2020). Due to the design of the solution concept as a generic SSI system consisting of the issuer, holder, and verifier, the system might be transferred to numerous certification processes. Other documents issued by public and private organizations could use this system to digitalize the process. Therefore, based on the learnings during the development, implementation, and evaluation of the artifact, we propose the following nascent design principles. These principles aim to extend the body of knowledge regarding best practices in designing SSI applications (Wang & Filippi, 2020).

Design Principle 1: Use the multiplicity of roles of actors for scaling the identity ecosystem

SSI represents a peer-to-peer system for IdM (Preukschat, 2021). Therefore, there are no longer dedicated servers (certificate authorities) and clients (users) (Cao & Yang, 2010). This is where the design of SSI systems differs from centralized systems, where the roles typically are defined when the system is set up. Rather, in an SSI system, all actors can transact with each other either as an issuer, holder, or verifier, while the configuration might even change over time (Mühle et al., 2018). To take full advantage of SSI, such systems should be designed so that one party can take on each of the three named roles at any time.

In the present case, we encounter this phenomenon in the design of the tax authority system. The tax authority is an issuer of credentials and has to verify the retailer's identity VC. This fact required several considerations. First, the tax authority's system became more complex, as it must now cover the issuance process of the tax VC and the verification process of the identity VC. Second, additional governance guidelines had to be considered as we needed to define which identity VCs should be trusted. Thinking beyond the processes presented in this article, the tax authority could also be the holder of identity attributes, i.e., VCs. For example, other governmental institutions could issue credentials to the tax authority authorizing it to provide certain services. A citizen or company could then request proof of this certificate from the tax authority beforehand. This would, in turn, increase the technical effort and require even more multi-level governance measures. However, it would also allow making use of a web of trust, creating a decentralized fault-tolerant authentication for DIDs and public keys, very similar to the approach implemented by Pretty God Privacy, also known under its abbreviation PGP (Garfinkel, 1995).

Based on our findings, we suggest that regulators in the future make their identity frameworks more flexible. For example, eIDAS does not provide for overlapping roles but instead requires a rigorous audit process first before acting as an issuer or verifier. While this makes sense in highly regulated applications, it potentially hinders the growth of use cases and, thus, the entire ecosystem. Overly strict regulation of SSI and its roles would potentially prevent the promises of flexibility and interoperability from being delivered.

Design principle 2: Consider credentials for multiple applications to facilitate additional use cases

Like in the analog world, VCs can be issued without a specific application in mind but rather as a general-purpose

document. For example, issued one time, the underlying identity information can be used in a wide range of different scenarios. Thanks to its portability, the same holds for SSI credentials (Mühle et al., 2018). As such, multiple uses of a credential for services reduce friction and improve user experience (Wang & Filippi, 2020).

We made use of this principle by allowing the retailer to apply for their master identity at the citizens' office. Once they receive their identity VC, they use it for two different services. First, they use it for providing identity information and as a means of authentication towards the tax authority. Second, together with tax VC, they employ the identity VC to provide identifying information for the marketplace. The blockchain spans a decentralized, organization-overarching infrastructure for public DIDs and revocation lists. This property allows any organization, regardless of whether public or private, to validate and compute the respective identity information. In the future, additional services can make use of the VCs issued in the given case. E.g., a bank could join the SSI system. They could then use the identity and the tax VC to perform know-your-customer procedures, including the certainty that the retailer has a valid tax registration.

Once again, we would like to plead for a flexible design of future identity ecosystems. Only if these ecosystems are as open and interoperable as possible can new applications successively build on them. This also means that the development of new systems and the corresponding regulatory framework should not be based directly on fixed use cases but should also allow for organic developments. Therefore, VCs should not be designed from the outset only for specific applications but should be made usable in a context-independent manner.

Design principle 3: Recognize the identity holder as the primary controller to ensure seamless processes

What might sound rather obvious in a system where the user stands in the middle of any interaction drastically restricts the way processes can be planned. All processes either start with action from the identity holder or need their approval at a certain step. Therefore, applications using SSI must be designed to consider the identity holder an active part in almost all processes.

In the given case, the online retailer must be involved in many actions, resulting in numerous interactions. They must accept new connections, credential offers, and proof requests and actively manage presentations. We later realized that proof of non-revocation by design is an active process as well, always involving the retailer (Mühle et al., 2018). That means that when a retailer is no longer registered, the marketplace neither gets automatically informed about that fact nor can it perform periodic checks. Therefore, we later decided that we had to require the retailer to perform proof of non-revocation periodically. We also considered automation of this process after initial consent from the retailer. However, we dismissed this approach during our development phase as it might be questionable to what extent such a level of automation is in line with SSI's basic philosophy (Preukschat, 2021). In his work about privacy self-management, Solove (2012) describes that users tend to give general consent to disclosing data out of convenience, neglecting the associated privacy risks. Therefore, automation could quickly lead to a situation in which the user no longer has an overview of the consent declarations and loses control over their or her identity. For business reasons, a retailer may prefer to cease operations, so the marketplace would never have to know about the revocation of its tax VC. Automatic retrieval of the revocation by the marketplace could lead to the retailer unwillingly disclosing this information. The decision not to automate the proofing process was also supported by the fact that the wallet implementations we considered do not allow automation of this process but always require active user participation.

SSI provides for the holder to be placed in the center of all activities. In addition to the aforementioned need for more flexible regulation, this means a heavy responsibility burden for the holder in the future. Government and regulators will therefore have to conduct a strong education of individuals as well as companies to ensure that they can use the new opportunities without risk.

Design principle 4: Use public DIDs only for credential issuers to minimize privacy issues

DIDs are an important measure within the SSI stack to support the communication and identification of parties within the identity ecosystem. Generally, DIDs can be made public (i.e., public DIDs) by publishing the respective DID Document on a Verifiable Data Registry or kept private by exchanging it and its DID Document bilateral. Following the general perception of using the blockchain only when and where necessary (Rieger et al., 2019), we propose to use public DIDs only for credential issuers. For all other parties, bilateral exchange of the required data is sufficient. Being able to freely decide whether to write an identifier on the blockchain or keep it private is a major differentiator compared to other blockchain-based IdMs, where all identifiers are stored on the blockchain (Dunphy & Petitcolas, 2018; Faber et al., 2019; Sullivan & Burger, 2017).

We applied this design principle by only publishing the DIDs and DID Documents of the two issuing parties, namely the tax authority and the citizens' office. This allows any party later to look up their DID Documents on the blockchain, resolving the respective signing keys and, thus, verifying the signature of VCs. The online retailer and the marketplaces do not issue VCs. Therefore, we decided to

exchange their DIDs and DID Documents only bilaterally. This approach has two major benefits. First, it reduces the number of transactions that need to be written on the blockchain. Reducing required transactions is considered a best practice for designing blockchain-based solutions (Rieger et al., 2019). Second, it also prevents the risk of publishing personally identifiable information on the blockchain, potentially infringing GDPR requirements. This is especially important if the online retailer acts as a private person and not as a natural person.

While this is a simplification for the holder and the verifier, issuers need to overlook their public closely DID. Accordingly, issuers should regularly check the accuracy and timeliness of their data on the blockchain. This is the only way to ensure that the relevant endpoints can be reached and that issued VCs can be verified.

Conclusion

This study comprises the conceptual design, prototypical implementation, and evaluation of a blockchain-based SSI system that incorporates a set of public and private organizations to verify the tax registration of online retailers. First, the existing processes were analyzed, and the potential for improvement was identified. The paper-based process currently shows significant inefficiencies due to media discontinuities and counterfeiting risks. Second, an SSI solution was proposed that integrates into the existing system landscape and issues VCs to online retailers. They can then use a digital wallet to present their registration and general identity information to the marketplaces. The validity can be checked via a registry on a public blockchain. Communication occurs mostly via a bilateral link between the parties involved (citizens' office, tax authority, online retailers, and marketplaces) and in the form of VPs. Finally, we extensively evaluated the overall concept and proposed four design principles to develop SSI-based applications.

By presenting the artifact, giving insights into the design and development process, evaluating the artifact, and proposing design principles, this paper seeks to make the following contributions. First, we provide practical insights into our design for an improved IdM spanning across various organizations and highlight the underlying decisions that support similar efforts in e-government systems and the public sector. To our best knowledge, this is the first paper describing in detail an SSI system for supporting taxation-related processes in a business-to-business environment, thus demonstrating potential also beyond frequently discussed use cases like university diplomas or driver's licenses. Abstracting from the given use case, we are convinced that the detailed insights into the processes and technical functionalities will also provide knowledge for the development of similar systems also beyond taxation applications. Second, our evaluation sheds light on the effectiveness of such a system in supporting inter-organizational processes. In particular, we demonstrate the benefits and hurdles of the use of SSI. Finally, we answer the call of Nærland et al. (2017) and Carter and Ubacht (2018) and provide general guidelines that contribute to the design theory of blockchain-based IdM, specifically SSI. We hope that our design principles will ultimately lead to more effective blockchain-based SSI applications.

This study has limitations. The design was carried out in the form of a proof of concept to evaluate the general feasibility. However, the scope of the implementation and the interviewees were limited to the tax authority. We propose involving various stakeholders, including online retailers and marketplaces, to analyze technical, socio-technical, and socio-economic aspects in real conditions, offering opportunities for additional evaluation in future research. Furthermore, our discussion of this study points out the benefits of opening the system to other use cases. However, this idea is only theoretically driven as of now. The combination of issued proofs of different parties and inter-organizational collaboration must be evaluated empirically to demonstrate its real value. This would also allow better use of ZKPs, including anonymous VCs and range proofs, which will be urgently needed to ensure privacy in many applications. Finally, future research should expand on the political, legal, and ethical implications of SSI and the impact of these non-technical factors on the success and adoption of SSI in organizations and institutions.

Despite the aforementioned limitations, this paper shows that blockchain and SSI can benefit public and private organizations alike. The research project demonstrates the applicability and effectiveness of such systems for inter-organizational IdM. Thus, we hope that the results of this paper contribute to an emerging SSI ecosystem.

Acknowledgement We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their support of the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" as well as the Bavarian State Ministry of Digital Affairs and the Bavarian State Taxation Office for their support of the project "SSI@LfSt" that made this research possible.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data Availability The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to them containing confidential information or information that could compromise research participant consent.

References

Allen, C. (2016). *The path to self-sovereign identity*, available at http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html. Accessed 3 Dec 2022.

Arnold, L., Brennecke, M., Camus, P., Fridgen, G., Guggenberger, T., Radszuwill, S., Rieger, A., Schweizer, A., & Urbach, N. (2019). Blockchain and initial coin offerings: Blockchain's implications for crowdfunding. In H. Treiblmaier & R. Beck (Eds.) *Business Transformation through blockchain* (pp. 233–272). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-98911-2_8.

Baskerville, R., Baiyere, A., Gergor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a Balance between artifact and theory. *Journal of the Association for Information Systems, 19*(5), 358–376. https://doi.org/10.17705/1jais.00495.

Bitnation. (2017). *BITNATION and Pangea Documents, resources and contributor guidelines*, available at https://github.com/Bit-Nation/Pangea-Docs. Accessed 26 Jul 2022.

Byun, D. H., & Finnie, G. (2011). Evaluating usability, user satisfaction and intention to revisit for successful e-government websites. *Electronic Government, an International Journal, 8*(1), 1. https://doi.org/10.1504/EG.2011.037694.

Camenisch, J., & Lysyanskaya, A. (2002). Dynamic accumulators and application to efficient revocation of anonymous credentials. *Annual International Cryptology Conference*, 61–76. https://doi.org/10.1007/3-540-45708-9

Cao, Y., & Yang, L. (2010). A survey of identity management technology. *2010 IEEE International Conference on Information Theory and Information Security,* Beijing, China. 2010, IEEE, 287–293. https://doi.org/10.1109/ICITIS.2010.5689468.

Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated identity architecture of the European eID system. *IEEE Access, 6*, 75302–75326. https://doi.org/10.1109/ACCESS.2018.2882870

Carter, L., & Ubacht, J. (2018). Blockchain applications in government. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age,* 1–2. https://doi.org/10.1145/3209281.3209329

Caza, B. B., Moss, S., & Vough, H. (2018). From synchronizing to harmonizing: The process of authenticating multiple work identities. *Administrative Science Quarterly, 63*(4), 703–745. https://doi.org/10.1177/0001839217733972

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks, 37*(2), 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1

Decentralized Identity Foundation. (2021). *GitHub - Decentralized-identity/universal-resolver: Universal Resolver implementation and drivers*, available at https://github.com/decentralized-identity/universal-resolver. Accessed 12 Dec 2022.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity - Opportunities and challenges for the digital revolution. *arXiv preprint.* https://arxiv.org/abs/1712.01767

Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE security & privacy, 16*(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless networks*, 1–11. https://doi.org/10.1007/s11276-018-1883-0

EUR-Lex. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,* available at http://data.europa.eu/eli/reg/2014/910/oj. Accessed 5 Jan 2022.

European Commission. (2020). *The Commission has launched a public consultation on the revision of the rules on electronic identification and trust services for electronic transactions in the internal market, the eIDAS Regulation*, available at https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation. Accessed 31 Jul 2022.

European Commission. (2021). *Study to support the impact assessment for the revision of the eIDAS regulation*, available at https://op.europa.eu/en/publication-detail/-/publication/9ce0f9e5-03bb-11ec-8f47-01aa75ed71a1/language-en/format-PDF/source-225913375. Accessed 5 Dec 2022.

Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019). BPDIMS:A blockchain-based personal data and identity management system. In Bui, T. (Ed.), *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.821.

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access, 7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L., & Shi, W. (2018). Blockchain-based identity management with mobile device. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 66–70. https://doi.org/10.1145/3211933.3211945

Garfinkel, S. (1995). *PGP: Pretty Good Privacy*. Sebastopol: O'Reilly Media, Inc.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01.

Guggenberger, T., Schweizer, A., & Urbach, N. (2020). Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology. *IEEE Transactions on Engineering Management, 67*(4), 1074–1085. https://doi.org/10.1109/TEM.2020.2978628

Haddouti, S. E., & Ech-Cherif El Kettani, M. D. (2019). Analysis of identity management systems using blockchain technology. *International Conference on Advanced Communication Technologies and Networking (CommNet)*, 1–7. https://doi.org/10.1109/COMMNET.2019.8742375.

Hyperledger Aries. (2020). *hyperledger/aries*, available at https://github.com/hyperledger/aries. Accessed 27 Dec 2022.

Hyperledger Indy. (2020). *hyperledger/indy-sdk*, available at https://github.com/hyperledger/indy-sdk. Accessed 27 Dec 2022.

Jensen, J. (2012). Federated identity management challenges. *2012 Seventh International Conference on Availability, Reliability and Security,* Prague, TBD, Czech Republic, IEEE, 230–235. https://doi.org/10.1109/ARES.2012.68.

Lesavre, L. (2020). *A taxonomic approach to understanding emerging blockchain identity management systems* [White paper].

National Institute of Standards and Technology, p. 62. https://doi.org/10.6028/NIST.CSWP.01142020.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K.-K.R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications, 166*, 102731. https://doi.org/10.1016/j.jnca.2020.102731

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS Quarterly,* 725–730. https://doi.org/10.2307/25148869

Marina, N., Taskov, P., & Karamachoski J. (2020). Blockchain-based application for certification management. *Tehnički Glasnik, 14*(4), 488–492. https://doi.org/10.31803/tg-20200811113729

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*, Klagenfurt, Austria, available at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173. Accessed 12 Dec 2022.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nærland, K., Müller-Bloch, C., Beck, R., & Palmund, S. (2017). Blockchain to rule the waves - Nascent design principles for reducing risk and uncertainty in decentralized environments. *Proceedings of the International Conference on Information Systems (ICIS)*. http://aisel.aisnet.org/icis2017/HCI/Presentations/12/

Nauta, J., & Joosten, R. (2019). *Self-Sovereign Identity: A comparison of IRMA and Sovrin,* available at https://publications.tno.nl/publication/34634504/uwmOQq/TNO-2019-R11011.pdf. Accessed 12 Dec 2022.

Nunamaker, Jr., J., F., Minder, C., & Titus, D., P. (1990). Systems development in information systems research. *Journal of management information systems*, 89–106. https://doi.org/10.1080/07421222.1990.11517898

Páez, R., Pérez, M., Ramirez, G., Montes, J., & Bouvarel, L. (2020). An architecture for biometric electronic identification document system based on blockchain. *Future Internet, 12*(1), 10. https://doi.org/10.3390/fi12010010

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Preukschat, A. & Reed, D. (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Shelter Island: ManningPublications

Rathee, T., & Singh, P. (2021). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2021.03.005

Rhie, M.-H., Kim, K.-H., Hwang, D., & Kim, K.-H. (2021). Vulnerability analysis of DID Document's updating process in the decentralized identifier systems. *2021 International Conference on Information Networking (ICOIN)*, 517–520. https://doi.org/10.1109/ICOIN50884.2021.9334011.

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a blockchain application that complies with the EU General Data Protection Regulation. *MIS Quarterly Executive, 18*(4), 263–279. https://doi.org/10.17705/2msqe.00020.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*, 1880.

Sourabh, W. (2019). *Decentralized digital identity management using blockchain and its implication on public sector*, available at https://www.semanticscholar.org/paper/Decentralized-digital-identity-management-using-and-Wadhwa/9b6e9bd362dfa6182e833358c34b2ec60cf170cd. Accessed 26 Jul 2022.

Squicciarini, A. C., Czeskis, A., & Bhargav-Spantzel, A. (2008). Privacy policies compliance across digital identity management systems. In Bertino, E., & Damiani, M. L. (Eds.), *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS* (pp. 72–81). Irvine California. 04 11 2008 04 11 2008. New York: ACM. https://doi.org/10.1145/1503402.1503416

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review, 33*(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016

Treiblmaier, H., & Beck, R. (Eds.). (2019). *Business transformation through blockchain*. Springer International Publishing.

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-Sovereign identity solutions: The Necessity of blockchain technology. *arXiv preprint*. https://arxiv.org/abs/1904.12816

W3C. (2021a). *Decentralized Identifiers (DIDs) v1.0*, available at https://www.w3.org/TR/did-core/. Accessed 24 Apr 2022.

W3C. (2021b). *Verifiable Credentials Data Model 1.0*, available at https://www.w3.org/TR/vc-data-model/. Accessed 24 Apr 2022.

Wang, F., & Filippi, P. de. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain, 2*. https://doi.org/10.3389/fbloc.2019.00028

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Boston: Course Technology Press.

Williams, I. (2020). Cross-chain blockchain networks, compatibility standards, and interoperability standards: The case of European blockchain services infrastructure. *Cross-Industry Use of Blockchain Technology and Opportunities for the Future* (pp. 150–165). IGI global. https://doi.org/10.4018/978-1-7998-3632-2.ch010

Yavuz, E., Koc, A. K., Cabuk, U. C., & Dalkilic, G. (2018). Towards secure e-voting using ethereum blockchain. *2018 6th International Symposium on Digital Forensic and Security (ISDFS),* Antalya. 2018, IEEE, 1–7. https://doi.org/10.1109/ISDFS.2018.8355340

Zambrano, R., Young, A., & Verhulst, S. (2018). Connecting refugees to aid through blockchain-enabled ID management: World Food Programme's building blocks. *GovLab October*, available at https://www.irisguard.com/media/laglvgzk/building-blocks-case-study.pdf. Accessed 12 Dec 2022.

Zhu, X., & Badr, Y. (2018). A Survey on blockchain-based identity management systems for the Internet of Things. *IEEE International Conference*, 1568–1573. https://doi.org/10.1109/Cybermatics_2018.2018.00263