Ziegler *et al.*
EURASIP Journal on Information Security (2025) 2025:12
https://doi.org/10.1186/s13635-025-00195-6

EURASIP Journal on Information Security

RESEARCH Open Access

Designing a security incident response process for self-sovereign identities

Leonhard Ziegler[1], Michael Grabatin[1], Daniela Pöhn[1*] and Wolfgang Hommel[1]

Abstract

While self-sovereign identities (SSI) have been gaining more traction, the topic of SSI security has yet to be addressed. Especially regarding response procedures to security incidents, no prior work is available. However, incident response processes are essential to systematically respond to a security incident in a timely manner. We first evaluate the current state-of-the-art by conducting a literature survey and contacting organizations that offer SSI. The insights underpin the subject's relevance, highlighting that incident response capabilities are just starting to be developed. Contributing to this development, we identify the challenges of building a security incident response process for SSI. Mainly, the decentralized nature inhibits the utilization of known best practices, which all focus on building a centralized incident response capability. However, even in the case of SSI, some centralized entities may exist. Therefore, we design two variants of SIR processes: one more centralized and one more decentralized. For the latter, the problem size is reduced in the first step by identifying all the stakeholders within an SSI ecosystem and then analyzing possible proactive and reactive measures each participant can access. This procedure leads to the grouping of SSI system participants into three distinct domains of incident response. For each domain, different capabilities for handling incidents are introduced depending on the involved stakeholders, their infrastructure, and their goals. To demonstrate the procedures, incident scenarios for each domain highlight the workflows during incident handling.

Keywords Self-sovereign identity, SSI, Identity management, Security incident response, SIR, Security

1 Introduction

With an increase in cyber attacks, the amount of data exposed by adversaries increases. The exposure or compromise of data, such as India's Aadhaar System, with billions of records including names, email and physical addresses, phone numbers, and photos [1, 2], does not necessarily imply that they are utilized for fraudulent purposes. However, criminals sell personal data online that can be used for identity theft. One recent example is the Genesis market, which was taken down in the so-called Operation Cookie Monster [3]. The investigation showed that 1.5 million information packages were sold on the platform to be used for stealing social media profiles and emptying investment portfolios, bank accounts, and crypto-wallets of victims.

In order to decrease the impact of data breaches, decentralized approaches are being developed in the field of identity management (IdM). These so-called self-sovereign identities (SSI) typically utilize distributed ledger technologies (DLTs), such as blockchain. Other, more traditional forms of storage, trust, and protocols than those applied by, for example, Hyperledger and Sovrin, might be used in such a decentralized setting. One key element is, however, the storage of identity-related data. By storing identity-related data (*claims*) in wallets, every user is the ultimate owner of their data. Several aspects of SSI are planned to be introduced to European electronic identity (eID) with the new electronic Identification, Authentication and Trust Services (eIDAS) regulation [4]. The new concept also has new potential for cyber threats targeting these systems. As SSI is not yet widely deployed, little is

*Correspondence:
Daniela Pöhn
daniela.poehn@unibw.de
[1] RI CODE, University of the Bundeswehr Munich, Werner-Heisenberg-Weg 39, Neubiberg 85579, Bavaria, Germany

known about its possible practical security implications. First approaches try to analyze the threats to SSI based on distributed ledger technology (DLT) [5–8]. However, when security incidents appear, they have to be handled and mitigated systes more control and responsibility by exercising self-sovereign control omatically and in a timely manner. Compared to traditional IdM, the user receives more control and responsibility by exercising self-sovereign control over the claims stored in the wallet. This newly gained control might mean contributing to security incident response (SIR) processes, no matter which and how the underlying technologies and protocols are chosen.

Hence, in this article, we provide an overview of possible security incidents based on existing literature. We summarize a small-scale survey for SIR in the SSI context. Next, we analyze the governance structures of SSI to outline possible SIR processes that can handle the identified security incidents. This analyze is divided into a complete decentralized structure and an architecture with a centralized entity. The SIR processes can be applied independently of the underlying technology. Thereby, the new eIDAS regulation could facilitate the designed SIR processes. As centralized processes, according to standards, are already deployed and used in practice, we focus the evaluation on decentralized processes. These are evaluated based on the prototypically application of possible security incidents.

Contribution: (1) survey on SIR processes for decentralized settings with a specific focus on SSI, including interviews with organizations operating self-sovereign identity (SSI); (2) design of decentralized and centralized SIR processes based on the governance structures and architectures of SSI and the capabilities and responsibilities of the entities involved; and (3) evaluation of the SIR processes by prototypically playing security incidents.

The remainder of the paper is as follows: first, we outline the background and related work in Section 2. Section 3 summarizes the survey conducted by analyzing related work and interviewing organizations with existing SSI solutions. The applied method for designing centralized and decentralized SSI SIR is outlined in Section 4. We first design a centralized SIR process with a trusted third party (TTP) in Section 5. Then, we design decentralized processes divided into the different responsibilities and roles in Section 6. Next, Section 7 evaluates the decentralized SIR processes by prototypically playing selected security incidents. In Section 8, we discuss our approach before we conclude the paper with a summary and an outlook.

2 Background and related work

This section provides the background and a summary of related work. First, we outline traditional IdM (see Section 2.1) to show the current state-of-the-art in practice. Next, we provide the background to SSI (see Section 2.2). This is followed by an overview of security threats to SSI (see Section 2.3) and SIR processes in general (see Section 2.4). Both sections serve as a basis for the SIR processes for SSI (see Section 2.5).

2.1 Traditional identity management protocols

According to Carblanc [9], an identity management system (IdMS) is a set of processes and tools to establish the identity of a user in a system and control their access to resources based on the user's permissions and restrictions. Consequently, IdMS have to provide identification, verification, authentication, and authorization in centralized or cross-organizational contexts, i.e., centralized, federated, and user-centric IdM [10].

Centralized identity management A centralized IdM requires an IdMS, where the organization stores all identity-related data. This IdMS is, for example, used in organizations by utilizing directory services, such as lightweight directory access protocol (LDAP) [11] implementations. One widely adopted solution is Microsoft's Entra ID, formerly called Active Directory (AD). Often, single sign-on (SSO) is operated, allowing users to access all services within the organization with only one login per session.

Federated identity management In federated identity management (FIM), users can access services within the federation using the same digital identity. A federation is a circle of trust consisting of several organizations, specifically home organizations (identity provider) and services (service provider). This means, both entity types (identity provider and service provider) have to operate an implementation of the same protocol.

A typical protocol in research and education federations is security assertion markup language (SAML) [12]. These federations are operated by national research and education networks (NRENs), which serve as TTPs. SIR requirements and standards were introduced with the name of Security incident response trust framework for federated identity (Sirtfi), which is outlined in Section 2.5. Another example of SAML application is the current eID infrastructure.

Especially in web contexts, but also increasingly in former SAML federations, the protocols of Open Authorization (OAuth) [13] and OpenID Connect (OIDC) [14] are introduced. This is, for example, the case in eID by the new eIDAS 2.0 regulation that initiates the use of wallets and states the possible application of OAuth-based protocols. OIDC is built on top of OAuth, allowing for authentication. Both protocols are utilized in OpenID federation [15], a protocol draft allowing for the creation of federations in OAuth/OIDC settings. Other drafts developed by the OpenID foundation [16–19] try to establish interoperability between OAuth/OIDC and SSI, which is described in the next section.

User-centric identity management In user-centric IdM, the user becomes the central point within identity processes. This design intends to increase users' privacy by involving them in various actions. One example is the protocol of user-managed access (UMA) [20], which allows users to share data, such as health data or a travel calendar, with whom and under which conditions they choose. However, user-centric IdM is still not widely adopted. Based on the evolutionary identity models, SSI would be the next step.

2.2 Self-sovereign identities

Allen [21] formulated ten principles for SSI. Further elements are needed to move from the principles to a functional IdMS. In the following, we introduce the most common elements and protocols, as shown in Fig. 1.

Decentralized identifiers (DIDs) [22] are persistent identifiers, consisting of a uniform resource name (URN) that defines the scheme, an universally unique identifier (UUID) for the utilized DID method, and a namespace-specific identifier. A DID is part of a key-value pair pointing to a *DID document (DDO)*, which lists further specifications. *Claims* are statements about the subject (*the user/holder*), verified by an *issuer*. A *credential* consists of several claims and metadata, such as an identifier, the issuer's name, or an expiration date. These credentials and the corresponding metadata are cryptographically signed and issued as *verifiable credentials (VCs)* [23]. Theoretically, also *zero-knowledge proofs (ZKPs)* [24] are possible. ZKPs cryptographically prove a statement, such as age, without disclosing the original data of the holder to the *verifier*. These VCs and ZKPs with additional data are stored in applications on devices called digital *wallets*. Wallets can be software or hardware components, though software components, such as an app on a smartphone, are more likely. While the user interacts with the digital wallet, representation of the user is achieved by a digital *agent*. Edge agents operate locally in close proximity to the user, whereas cloud agents are hosted in the cloud. The concept of hosting a wallet and an agent can also be called an identity hub. To ensure that user data can be exported and synchronized between multiple hubs, multiple protocols are utilized, such as DID authentication (DIDAuth) [25] and DID communication (DIDComm) [26].

These elements are applied in workflows with the entities of holders, issuers, and verifiers. Issuers provide VCs to the holders. The holder stores any issued credentials in one or more digital wallets or identity hubs. The credentials are again signed but with the holder's DID. Hence, any party can verify that the holder signed the credential. Lastly, a verifier who is requesting proofs can receive a verifiable presentation of issued claims. The verifier can assert their origins since the holder and issuer sign the claims.

When discussing the architecture of SSI, the layers described by the Hyperledger Aries project [27] are often used (see Fig. 2). These are designed similarly to the Open Systems Interconnection (OSI) model layers. The lower layers consist of decentralized storage

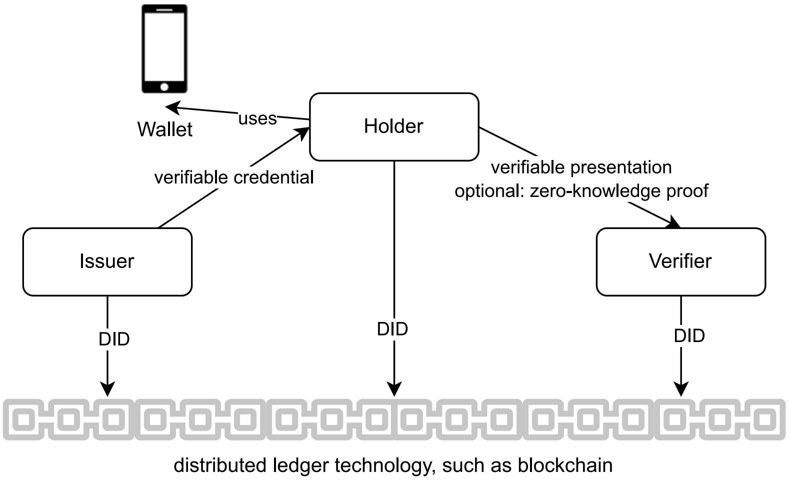

Fig. 1 Overview of the most important elements of self-sovereign identities

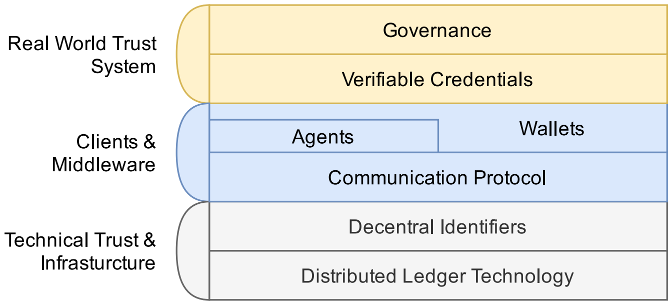

Fig. 2 Self-sovereign identity stack based on the Hyperledger Aries project [28]

and communication protocols. Layer five defines the processes for issuing, exchanging, and presenting VCs, whereas the top layer comprises the governance structure, which is relevant for SIR. The most common implementation as of 2023 is based on the SSI protocol, initially developed by Sovrin and continued as Hyperledger Indy (implementation of a permissioned DLT on layer one) and Aries (tools for generating and communicating VCs on layers two to four) by the Linux Foundation [27]. This SSI model also shows that the software and actual technology used in one layer can be changed.

As described in Section 2.1, new developments try to establish interoperability between OAuth/OIDC and SSI. Thereby, these protocols might be used to exchange claims, making both federated and self-sovereign identities possible. Also, other types of (decentralized) storage and trust, such as a public key infrastructure (PKI) and OpenID federation, might be applied. Consequently, a variant with only the introduction of a wallet might help provide the user with more control. Therefore, there might be scenarios with a centralized entity and those with a decentralized structure.

2.3 Threats to self-sovereign identities

Multiple approaches have been published focusing on the blockchain component in general. Hedayati and Hosseini [29] depict 34 attacks on blockchain networks, with the Bitcoin network as a reference point. Ahmed et al. [30] identify 12 network-based attacks specific to 38 academic SSI approaches. In relation to that, Guggenberger et al. [31] highlight the overrepresentation of popular public blockchains in the field of blockchain security analysis. Schlatt et al. [32] argue that since most approaches build on the assumption that they apply fully permissionless systems, scenarios in which at least a subset of nodes is trusted are disregarded. Kim et al. [33] group the technical components into five domains, which expose seven attack surfaces to DID workflows.

Schardong and Custódio [34] have identified 21 problems concerning SSI addressed by the literature they reviewed, of which only two are related to security, namely risk assessment and threat analysis. Naik et al. [5] address both, whereas Dingle et al. [35] examine the inherent security properties of verifiable credentials for a specific use case. Since then, a few more publications have targeted the security of SSI. Naik et al. [6], Grüner et al. [7], and Pöhn et al. [8] try to model the threats to SSI. Based on these publications and a literature review by Pöhn et al. [36], it becomes apparent that more threats than those described probably exist.

Possible threats to SSI and their assets include a malicious actor obtaining fake credentials, spoofing one entity, amending/stealing credentials, and obtaining personal data [5]. In the case of a malicious actor obtaining personal data (used in Section 7.1), the malicious actor may gain unauthorized access to the user's wallet by receiving user credentials and accessing the wallet. This attack could be done by using malware or a social engineering attack (receiving user credentials) and stealing the phone or gaining remote access to the wallet (accessing the wallet). The installed malware could grant remote access. In this case, the user and the other entities may start the SIR process. However, it might be required that the users provide information. As described above, this process is independent of the underlying technology. If an issuer or a verifier is compromised, then the signing keys have to be revoked as a minimum reaction (used in Section 7.2). Similarly, if TTPs are compromised that operate the network, then at least their signing keys have to be revoked (used in Section 7.3).

2.4 Security incident response processes

An event is any observable occurrence in a system or network, including a user connecting to a file share or a firewall blocking a connection attempt. If this event has negative consequences, such as system crashes, then it is called an adverse event according to National Institute of Standards and Technology (NIST) [37]. Following this, a security incident is a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. These security incidents have to be handled in a so-called security incident response. NIST describes a benefit of having such an incident response capability (e.g., in a team) as it supports responding to incidents systematically so that appropriate actions are taken. According to NIST [37], the incident response life cycle consists of the phases of (a) preparation; (b) detection and analysis; (c) containment, eradication, and recovery; (d) and post-incident activities. Furthermore, NIST emphasizes on the need of coordination and information sharing, especially if several entities are impacted. The type of coordination should be defined prior to any incident, whereas the information sharing might be ad hoc or partially automated during the incident response life cycle.

Governmental agencies, researchers, and the private sector have published a variety of standards, frameworks, and guidelines for incident management, such as ISO/IEC 27035 [38], NIST Special Publication 800-61 [39], and ENISA Good Practice Guide for Incident Management [40]. In research, SIR processes are analyzed and improved. Schlette et al. [41] provide an overview of incident response formats and playbooks to represent procedures. Ioannou et al. [42] highlight difficulties in communication and coordination based on a survey with 25 participants, whereas Redmiles [43] analyzed the cross-cultural aspects of end-users who recently had experienced suspicious login incidents on their Facebook (now: Meta) accounts.

2.5 Security incident response processes for self-sovereign identities

The standards, frameworks, and guidelines for incident management described above mainly concentrate on one central entity, though they provide information on multi-entity scenarios. In the context of FIM for the research and education inter-federation eduGAIN, Sirtfi [44] was developed by a dedicated Research and Education FEDerationS (REFEDS) [45] working group. It describes the requirements and processes for SIR in this specific federated setting (see Section 2.1 for the protocol involved).

Regarding SSI, incident response is not mentioned in any publication; regarding decentralized SIR, literature is scarce. Graf and King [46] propose a blockchain-based platform for automated incident classification and management. Whereas automating workflows during the assessment of security events implies timely reactions, their work is only a theoretical consideration. Adebayo et al. [47] design a blockchain network on top of Bitcoin for anonymous sharing of incident data and reaction strategies between affected organizations. The assumption of creating anonymity by using the Bitcoin network is questionable [48]. Similarly, [49–51] propose a blockchain-based trustworthy certification process for composite services, which can be applied to share incident-related information. However, the exchange process and power consumption of their chosen approach could be more efficient. Michail [52] elaborates on sharing incident-related data before introducing an incident reporting decentralized application. Putz et al. [53] design a blockchain security incident reporting system based on human observations (BISCUIT) in a decentralized finance (DeFi) network. The approach implies that a subset of organizations has enough stake in the network to invest in local reporting. In addition, it needs to be clarified how every user can participate based on knowledge and resources.

2.6 Summary

To conclude, several security threats exist and furthers still have to be explored, which implies that more work is required. In this article, we concentrate on the SIR processes. We found very little literature on decentralized SIR processes, but some on centralized SIR processes. These might be adaptable for an SSI setting with or without a TTP.

3 Survey on security incident response for self-sovereign identities

This section provides an overview of the literature review and the interviews conducted. We analyzed available resources, such as documents and guidelines of existing SSI implementations (see Section 3.1). Due to the lack of literature on SIR for SSI, we conducted a small-scale survey, interviewing organizations with existing SSI solutions (see Section 3.2). Lastly, we summarize the results of this section (see Section 3.3).

3.1 Literature review

Sovrin [54] was founded in 2016 as a non-profit organization. Since then, it has developed its own decentralized identity test and productive network based on an open-source framework managed by the Sovrin Foundation.

On a technical level, Sovrin utilizes an adapted instantiation of Hyperledger Indy, which the Sovrin Foundation administers on behalf of identity owners. Sovrin [27] defines three roles within its infrastructure: transaction authors, transaction endorsers, and stewards. The transaction author is an entity, such as the identity owner, that initiates a transaction. The transaction endorser is an organization authorized to authorize a transaction by digitally signing it. The signature is required so that the validator node accepts it. Unlike endorsers, transaction authors cannot change the ledger's state to allow for higher throughput. Hence, the transaction endorsers write transactions to the ledger on behalf of transaction authors. Stewards are organizations that must meet the qualifications and technical requirements defined by Sovrin's policies and that are approved by the Sovrin Foundation to operate a node. The nodes (i.e., validator nodes and observer nodes) are operated by stewards.

Some documents [55, 56] provide security guidelines and demands concerning SIR. The incident policy requires endorsers to maintain and follow documented SIR policies consistent with NIST guidelines, investigate unauthorized transactions and have an appropriate response plan, and notify and provide requested information to the foundation in case of security incidents. Thus, the policies are restricted to this role. However, further incident scenarios can occur and no communication plan is provided. Apart from Sovrin, other solutions include ShoCard [57] (evolving to PingOne Neo), uPort [58] (evolved to Serto and Veramo), Bitcoin [59], and Ethereum [60]. Regardless, we found no information related to security or SIR.

3.2 Interviews

In order to draw a sound conclusion on the practical relevance and state of deployment, we reached out to a subset of organizations that either conduct business or research in the field of SSI or decentralized governance. Note that SSI is still a developing field and the number of organizations being mature enough to answer the questions is low. The interview questions comprised questions related to the organization itself, security challenges and reactions to it, design decisions (such as the violations of the basic principles of SSI), governance structure, and the construction of incident response processes. The questions used as a guideline for the interview can be found in Section 10.

We received answers from IDunion [61], a project initiated around secure digital identities in Germany, and Netherlands TNO [62]. Both highlight the relevance of SIR for SSI while indicating that research is planned on the topic. According to the interview, IDunion is currently building an incident response plan (IRP) for its productive network. Its primary focus is issuing malicious code and General Data Protection Regulation (GDPR)-related data to the public readable ledger. The requirements for this process are mainly of a legal and business nature, while the technicalities are under discussion. Based on these observations, no general rule set for SIR exists.

3.3 Summary

To conclude, we found requirements for endorsers by Sovrin that are consistent with NIST guidelines (see Section 2.4). Apart from this role, we found neither documentation on security incidents nor information related to SIR processes. Other solutions did not provide further information. Based on the interviews, IRP is a relevant topic, though no SIR process exists yet (as of beginning of 2024).

4 Method for designing security incident response processes for self-sovereign identities

As the SSI concept and existing technologies on the subject are still at an early stage, a lack of SSI security standards is present. So far, we have noticed that literature on SIR for SSI is missing (see Section 2) and that organizations in the field are about to start working on that topic (see Section 3). Therefore, our purpose is to design SIR processes for SSI. We apply the following method, as shown in Fig. 3: (1) selecting SSI scenarios (see Section 4.1), (2) analyzing SSI architectures based on the scenarios (see Section 4.2), (3) designing the corresponding SIR processes (see Section 4.3), and (4) evaluating the decentralized SIR processes (see Section 4.4).

4.1 Selecting self-sovereign identity scenarios

In this section, we describe the step of selecting the self-sovereign identity scenarios based on the input of security threats and possible scenarios.

Input 1: security threats: as outlined in Section 2.3, few approaches [6–8] model the threats to SSI. Pöhn et al. [36] conducted a literature review on threats, showing that the publications do not contain all threats. For this analysis, we apply the threats outlined by Naik et al. [5]. As not the security threats but the processes are our focus, the preliminary status of the threat analysis is

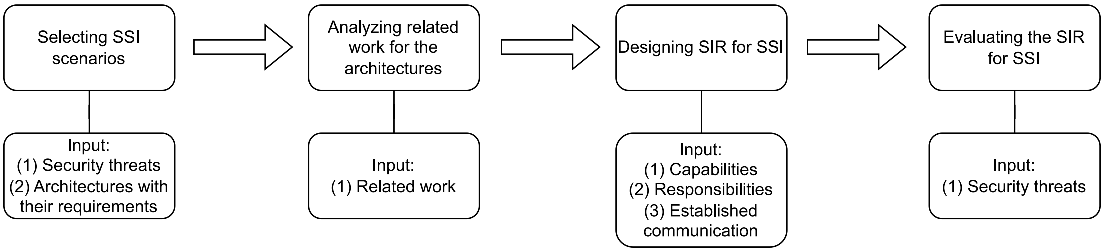

Fig. 3 Method for designing security incident response processes for self-sovereign identities

not an issue. Threats that will be identified in the future should work with our processes.

Input 2: architectures: as outlined in Section 2.2, although SSI is decentralized as introduced by Sovrin, there might be variants that utilize current FIM settings and, thus, be more centralized. In the case of the decentralized setting, there might be trust requirements that a consortium or similar body may define. However, the further communication might be decentralized. The more centralized setting can be seen as similar to a federation with a TTP. Therefore, we regard two main scenarios: (1) SSI with one or more TTPs and (2) SSI in a decentralized setting.

Scenario 1: self-sovereign identities with trusted third parties Imagine using an SSI wallet in a SAML federation or eID. Introducing the wallet gives the user self-sovereign control within the trust boundaries. As the federations typically use TTPs for governance and trust establishment, these entities remain in SSI. In addition, existing processes should be applicable. The underlying technologies might be the same as beforehand or with the addition of proxies or extensions as translators between the protocols. Even with pure SSI technologies, a TTP might be an appropriate place for governance.

Scenario 2: self-sovereign identities in a decentralized setting Imagine a consortium that wants to introduce SSI to establish cross-organizational IdM. They decide on protocols and implementations and deploy them in their infrastructures. In contrast to established federations with a TTP, they might work as a consortium to provide governance. Nonetheless, they must coordinate the following steps if a security incident occurs.

4.2 Analyzing related work for the selected scenarios and architectures

Based on the related work, as outlined in Section 2, and the architecture that is formed by the SSI scenarios, described previously (output of Section 4.1), we analyze the related work for the SIR processes fitting to the architectures and, hence, scenarios. We shortly summarize the input of this phase.

Input 1: related work: literature mainly focuses on centralized SIR processes. These might be adaptable for scenario 1, while taking the user into account. Concerning scenario 2, we found almost no related approaches. Additionally, this seems to be a practical issue according to the interviews, summarized in Section 3.2.

In the following, we outline our procedure depending on the SSI scenario.

Scenario 1: self-sovereign identities with trusted third parties Related work mainly designs SIR with centralized entities. For example, Sirtfi in FIM uses TTPs as coordinators. These approaches could be applied to SSI. However, even in SSI with TTPs, the user gains more control by the introduction of wallets.

Scenario 2: self-sovereign identities in a decentralized setting The overall issue is designing SIR for decentralized environments, while existing best practices are designed to work with centralized entities. Following this, no existing guidelines can be followed. As in FIM, there is a distinction between local and global incidents. These are further divided based on the SSI stack, shown in Fig. 2.

4.3 Designing security incident response processes for self-sovereign identities

As the related work, described in Section 4.2, mainly focuses on centralized structures, the capabilities, responsibilities, and communications serve as additional input for designing the SIR processes.

Input 1/2: capabilities and responsibilities: the responsibilities and capabilities within the related architectures are important inputs for the SIR process. If an entity, such as the holder, has responsibilities but not the capability to handle a security incident, then other entities may have to take over the responsibility. Hence, if these cases can be identified before designing the SIR processes, then they can be addressed accordingly in advance.

Input 3: established communication: established communication and communication means have to be taken into account as, at least, variants of the proposed solution. For example, if entities A and B know each other and share a threat intelligence platform, then a TTP does not have to coordinate the solving processes.

Scenario 1: self-sovereign identities with trusted third parties The differences described above must be identified, and the processes have to be designed accordingly, described in Section 5. The decoupling of issuer and verifier, as well as the introduction of the holder with a wallet or agent, provide challenges for the design phase.

Scenario 2: self-sovereign identities in a decentralized setting In a decentralized setting, the challenges of Scenario 1, trust, and coordination have to be addressed. Depending on the asset and responsibility, each participant has different goals for SIR. These processes are designed in Section 6.

4.4 Evaluating the security incident response processes for self-sovereign identities

For the evaluation in Section 7, we focus on the decentralized setting, as this scenario has the biggest difference to the current IdM world (see output in Section 4.3). We evaluate the designed SIR processes prototypically by selecting security threats.

Input 1: security threats: we select one security threat for each process. The security threats are based on those identified in Section 4.1.

Scenario 2: self-sovereign identities in a decentralized setting For the decentralized setting, security threats are selected. Based on this input, the designed processes are played step by step to evaluate the processes for missing and unnecessary steps and information. A special focus is set on coordination, as it was previously in Section 4.3 identified as a challenge.

5 Security incident response for self-sovereign identities with a trusted third party

As outlined in Section 4, there might be scenarios in which SSI, or at least elements of it, are applied in a more centralized setting. For example, they could provide governance or be used as trust anchors (such as PKI). Thereby, SSI is also supervised by one or a few authorities. This authority can subsequently act as a contact point and incident response team (IRT). Hence, we first outline Sirtfi, applied in FIM context, in Section 5.1, before analyzing its adaptability to centralized SSI in Section 5.2.

5.1 Sirtfi in federated context

Within FIM, Sirtfi [44] (see Section 2.5) was developed to provide a framework for coordinated SIR in federated settings with the underlying protocol of SAML (see Section 2.1). It can be applied in a single federation or within the inter-federation eduGAIN. These are established federations with federation operators acting as TTPs. Based on Sirtfi, the federation operator (TTP) acts as a coordinator within the federation case. If both affected entities (i.e., identity provider and service provider) have established contact prior to the incident, they can operate in that mode. However, they have to provide updates to the TTP. In inter-federation cases, both corresponding TTPs act as coordinators. Direct contact is possible in any case. The involved entities are responsible for the communication within the (internal) SIR process, but also the exchange of information, informing the management in specific predefined cases, and defining templates. A similar principle is applied for external communication, for example, with stakeholders and informing the holders. In addition, prevention (e.g., training, network and system security, and risk management) is necessary.

5.2 Designing security incident response for self-sovereign identities with a trusted third party

In this section, we analyze the roles and the architecture to design SIR processes for SSI with TTPs.

Trusted third party as coordinator The main role within Sirtfi has the TTP. Since TTPs are available in this scenario, they could be used as coordinators. For example, a TTP could be established similar to the federation operators. If no such organization exists, each entity could be part of a coordinated SIR team coordinating the SIR process. In this case, each entity has to provide staff, at least in case of an incident (ad hoc team). A permanent team could increase overall security. Similar to FIM, internal and external communication is needed within SIR processes. The documentation, analysis, prioritization, mitigation, recovery, and lessons learned can be done similarly to FIM. Depending on the applied protocols, the TTP may also be in control of the network (i.e., DLT).

Holder as involved entity The incident can be reported by various roles, including the SSI entities, employees, a help desk, the IT team, external news, and service providers, such as an Internet service provider. For resolution, information has to be gathered. The resources needed in this case depend on the actual infrastructure. In the case of proxies, the log files provide further data related to claims usage. With protocol extensions, this is different. In contrast to traditional FIM, the user stores more data by using the wallet. Hence, the coordinators or corresponding IRT team could guide the user into providing the necessary information. This could be utilized by a suitable graphical user interface (GUI) provided by the wallet. We also discuss this issue in Sections 6.3 and 8.

Summary In conclusion, the SIR for centralized SSI applies the best practices of centralized organizations and FIM. The issues of this scenario are the wallets being new items introduced to the infrastructure for holders with less knowledge about log files than entities. However, these wallets store relevant data for resolving security incidents.

6 Security incident response for decentralized self-sovereign identities

Based on Section 5, we know that the entities issuer and verifier are involved and that the holder has additional information though not the capability to react in a similar way as the professional entities. Furthermore, the network, such as a DLT, might be operated. Following this, we design SIR for three more decentralized SSI domains: the network SIR process (see Section 6.1), the issuer and verifier SIR process (see Section 6.2), and the holder SIR process (see Section 6.3). These are divided into responsibilities and corresponding processes. Lastly, we describe the communication strategy in Section 6.4.

6.1 Network security incident response process

Reflecting the SSI architecture, the single nodes and agents concerning infrastructure assets, key management and issuing data to the registry, and registry data concerning data assets are essential assets. Following this, the responsible parties for incident response are the node operators hosting the trust registry and the governance entity supplying the necessary frameworks and rule sets. As public-permissioned blockchain is currently likely to be applied in the context of SSI, we distinguish between reading data and submitting transactions to the ledger. Furthermore, we assume that a governance framework exists.

6.1.1 Architecture and responsibilities

For a network-wide SIR capability, the participants have to be specified.

Fully distributed security incident response In a fully distributed SIR, the node operators at which the security incident occurs would also take responsibility for an appropriate response by coordinating the SIR process. The response includes (1) estimating the impact of the incident on the network, (2) identifying other affected parties, (3) coordinating the formulation of an appropriate response and its implementation, and (4) writing the final report, which is propagated throughout the network. This way of organizing SIR suits infrastructures with a few highly skilled participants.

Hub-and-spoke security incident response In a hub-and-spoke model, a dedicated unit is established. This unit could consist of either unit members or a specific unit sponsored by the participants. Local security experts report incidents to a committee of experts, who find an appropriate response. One advantage is that communication with all network participants only takes place when sharing the final report. Another is that this approach scales better. Node operators are responsible for drafting and communicating an initial report to the global IRT. The global IRT could be a global non-profit organization, such as Sovrin, a national cooperative, an active community with its own set of governance structures, or a governmental body enforcing network regulations by law.

Governance body In either case, the network's governance body has to provide a technical and organizational policy to node operators that at least outlines the required security measures. In addition, local SIR capabilities, time intervals for internal audits, training, and further aspects may be specified. The policy may be adapted from Sovrin with adaptations based on the role and responsibilities. Node operators have to match the capabilities required for the corresponding SIR process that may be based on NIST Special Publication 800-61 [39].

6.1.2 Process of the network security incident response

The detection of a security event possibly qualifying as a security incident starts the network SIR process. This could be due to periodic system audits, breaches of security controls, reachability issues, or internal monitoring systems raising an alarm. For the global IRT, indicators of compromise include uncommon network scans, non-scheduled or prolonged downtimes of single nodes, non-participation or disturbances in the consensus algorithm, and concerns raised by external parties.

Network global SIRT Given a discovered security event at the node operator, it is reported to the local IRT team for an initial assessment in the context of the node operator's organization, as visualized in Fig. 4. The same applies to the initial assessment by the global IRT. Once an incident with a confirmed or suspected global impact is discovered, the local incident coordinator submits a report to the global IRT. For this, a template should be provided by the global IRT or governance body of the network. Based on [39, 44, 63], we compile a basic set of information to be included in an initial report: data and time of the security event; timeline of all actions carried out; containment steps undertaken so far; contact information of the responsible local incident coordinator; traffic light protocol (TLP) classification [64]; and incident details (i.e., physical location, cause and source, incident description, description of affected resources, estimated impact, details of compromised assets, and collected evidence). While node operators may not have all the information, the amount of detail influences their ability to analyze and handle the incident accordingly.

Node operator Once the global IRT receives information about a network security incident, it reviews the information so far gathered and further completes it to ensure that all potential threats and implications are

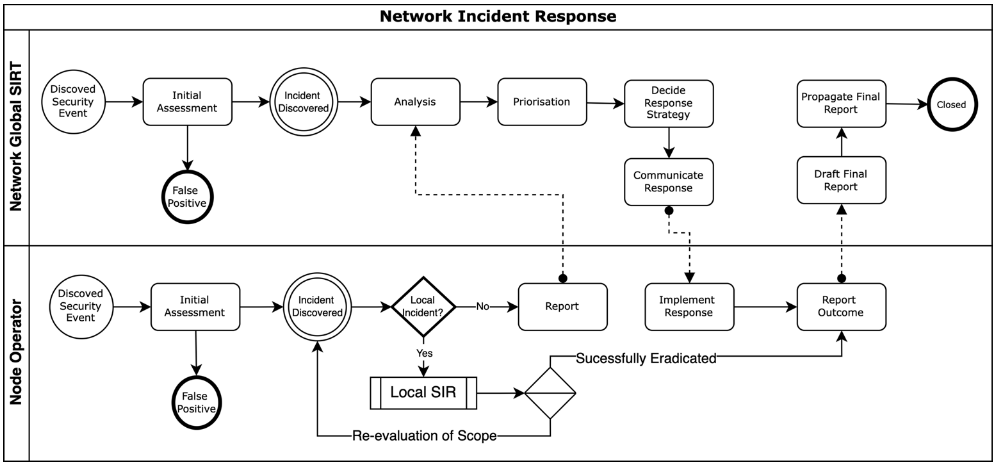

Fig. 4 Network level security incident response

included. The goal is to categorize the incident priorities to focus on available capabilities. Three scopes can be considered: functional impact, information impact, and recoverability. When this is achieved, response strategies can be formulated. This step aims to identify measures to contain and eradicate the incident so recovery becomes possible. Factors in choosing an appropriate strategy include the need for evidence preservation, maintaining service availability, available resources for implementation, and the effectiveness of the decided solution. As blockchain operates with a high level of redundancy, disconnecting a node should always be considered first. In the event that a majority of nodes with write privileges are compromised, non-validator nodes could be temporarily promoted until recovery can be conducted. Once a response strategy is decided, the teams' incident coordinators communicate it to the affected node operators. Next, the node operators have to implement the proposed measures. After successfully handling the incident, the node operator drafts a document detailing the outcome of the response process. This initial report sent to the global IRT can be used to compile the final report. Based on [39, 44, 63], the report should contain the following: the cause and classification of the incident; actions taken by all incident handlers; other incidents related to the incident; indicators related to the incident; impact assessment; a list of evidence gathered during the investigation; and comments from incident handlers. The final report is archived by the IRT and propagated to relevant parties.

6.2 Issuer and verifier security incident response

As the second SIR domain for SSI, the relevant actors are issuers, verifiers, and the governance entity. The goal of SIR in this domain is to ensure that incidents affecting specific entities and the trust relationship between these entities are effectively mitigated. Relevant assets are issuer infrastructure (for example, agents, authentication data, processes of issuing data, authentication of requesting parties, and key management) and verifier infrastructure (for example, agents and validation processes). A compromise of a verifier potentially leads to privacy concerns among the holders, whereas incidents affecting the integrity of issuers potentially affect IdM services across the entire network.

6.2.1 Responsibilities

Similarities and distinctions to network SIR Like the network SIR, the full responsibilities could be in the hands of the entity or by a global IRT. In order to enable multistakeholder coordination and provide a better outcome, we opt for a combination of both approaches. At least, coordination is outsourced to a dedicated hub, while incident handling remains the responsibility of the incident owner. However, the dedicated hub can provide its expertise to the incident owner if necessary. The main distinction between SIR in this domain and network SIR is the extent of locally available incident response capabilities. Whereas node operators are not required to invest in SIR capabilities for managing the entire SIR lifecycle, issuers must be able to conduct the entire handling for two reasons: (1) legal liabilities in case of abuse, fraud, or other misconduct and (2) existing resources, such as local IRT.

Entity's responsibilities Issuers are responsible for asserting that they have implemented an operational IRT according to the best practices of the governance entity accrediting the issuer. Concerning the responsibilities of the verifier taking on the role of a service provider from a traditional IdM point of view, the same responsibilities can be adopted. If ZKPs are applied, little personally identifiable information (PII) could get stolen from verifiers. The responsibility of the global IRT is to provide a point of contact for local incident coordinators. This ensures visibility of the incident's impact on the SSI system, as issuers cannot track a credential once it is issued to a holder. In addition, if several issuers notice a security incident, it may have a global impact. The coordinating team oversees appropriate measures from local entities to contain incidents by supporting the analysis and response steps if necessary and by providing report templates. Lastly, it is responsible for drafting the final report.

6.2.2 Process of the entity security incident response

The process of the entity SIR is based on Sirtfi [44] and its description by the German research network DFN [65]. It is applicable since the basic structure of roles and responsibilities is similar. However, to fit the context of SSI, the role of the coordinating team has shifted from inter-federation communication to evaluating the scope of an incident in a more detached environment. The process is outlined in Fig. 5.

Affected participant When a potential incident affecting IdM-related services is discovered, a report is submitted to the local IRT. The local IRT assesses the potential incident to rule out false positives or confirm the incident. Initial means can originate from various sources, including monitoring software, network and operating system logs, and users experiencing problems. If the incident impacts other entities' IdM-related services, a report must be submitted to the coordinating team. Depending on the available knowledge at that time, the report itself can be minimalistic as long as it contains a brief summary of events and assessment steps. The format should be based on a template, which includes the TLP classification. Once the global coordinating IRT is notified, it offers assistance in analyzing and responding to the incident. For example, it reviews reports and checks final reports for similar incidents. Multiple incoming reports are evaluated for overlapping aspects. All communication taking place during coordination is documented in

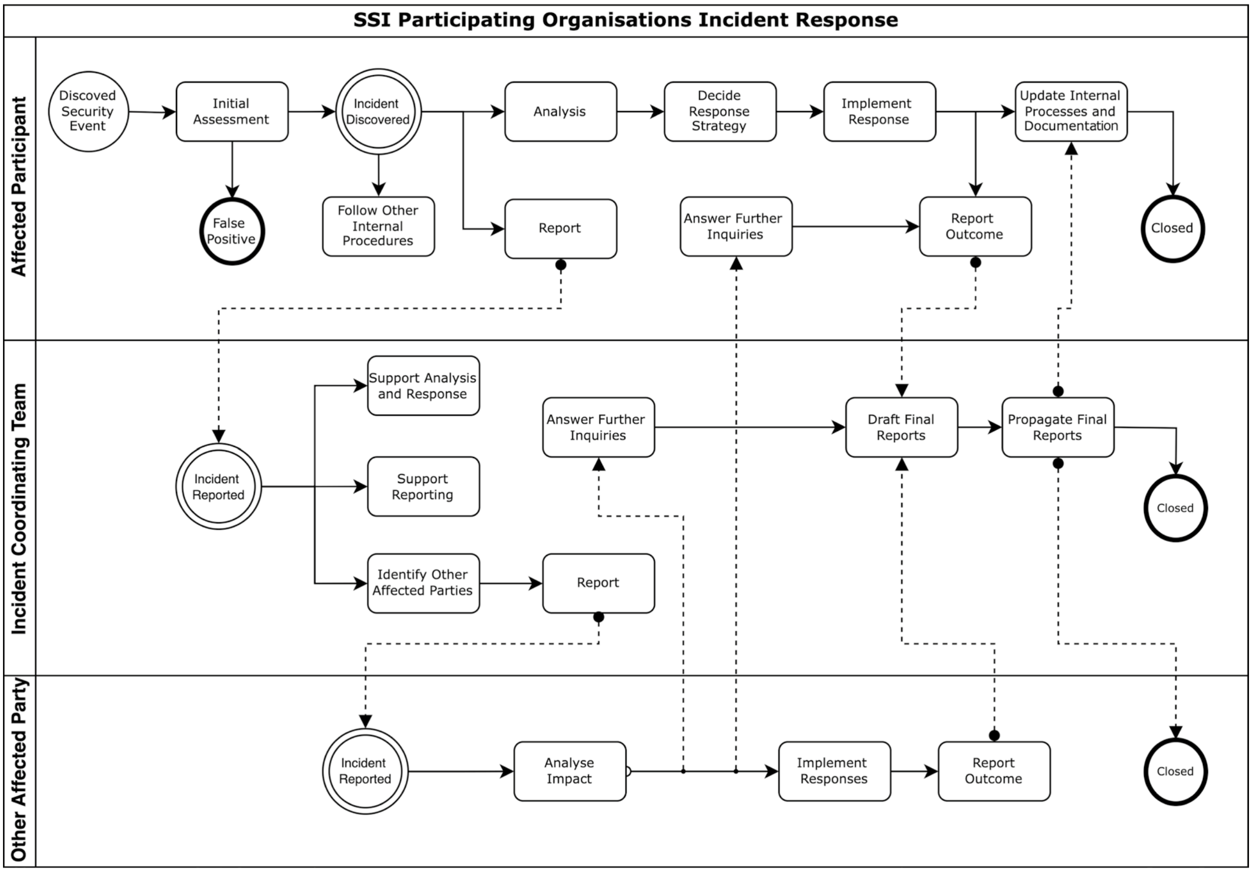

Fig. 5 Entity level security incident response

the final report. Next to providing support, the primary responsibility is evaluating the extent of the incident to identify other affected entities.

Incident coordinating team If the local IRT successfully discovers an incident after initial assessment, the same analysis, decision, and response steps are conducted as in a network SIR. Additionally, the affected organization may take further steps in compliance with internal incident management procedures. During these procedures, the affected entity has to comply with their incident owner's responsibility by answering inquiries and updating the global IRT. After the incident is successfully eradicated, an outcome report is submitted by all affected entities. For this purpose, a template is provided by the global IRT. Based on these reports, the global IRT drafts a final report detailing the scope of the incident and distributes it to the affected entities. Based on this report, the affected entities can revise existing internal processes related to incident handling.

6.3 Holder security incident response

Lastly, we outline the holder SIR, the most significant difference from the current IdM, as the holder is in self-sovereign control. Thereby, the holder has information about the security incident. However, their response capabilities are limited.

6.3.1 Responsibilities

Whereas a formal process was defined for both previously described domains, this is not feasible for the holder's domain. The distinction resides in the available capabilities: holders, by default, are not involved in IRT in the context of the model. No substantial knowledge relating to incident handling can be expected from the average holder. At this point, the extent of decentralization becomes apparent. Due to the holder's self-sovereignty, they are ultimately responsible for their data and, hence, the appropriate reaction to events threatening their security. However, existing approaches for SIR do not consider single users to be in control of their data. Hence, holders depend on the functionality provided to them by wallet developers to control their setup. As a corollary, wallet developers and holders are the two key players within this domain. Both are responsible for the holder's infrastructure and the stored data, processes to obtain the wallet, issue data, authenticate, wallet proof control, key management, and selective disclosure.

6.3.2 Process of the holder security incident response

For our purpose, we define the SIR capabilities of holders by evaluating existing wallet control functionalities as far as current state-of-the-art wallets allow. Given that identity wallet security specifications are recently starting to be published (see [66, 67]) or still need to be finalized (see [68]), this task proves challenging. Furthermore, wallet SIR capabilities are not defined in any of these standards. We found no such functionality when testing current SSI wallets available in the Google Play Store. The main aspects of control a holder has are revocation and recovery. The first ensures that in the event the wallet gets stolen and can be accessed by an attacker, it cannot be used to access existing trust relationships. On the other hand, recovery limits the impact of inaccessibility so that digital identities are not permanently lost. The wallet itself is only a data container that holds records. Standards do not fully address both functionalities since they require interactions with other architectural components. Furthermore, the user mainly interacts with the GUI. Since these do not follow specific rules, the functionality is either not fully implemented, is not convenient, or contradicts the decentralized aspect [69]. Based on these observations, we see urgent future work in case the holder is involved in SIR.

6.4 Communication strategy

For communication between the IRTs, a dedicated incident coordinator is appointed. As the trusted registry already provides a means for organizations to publish a DDO containing service endpoints, we publish the incident coordinator's contact details or methods of contact alongside other data. With this, encrypted email communication is already possible. Other traditional means of contact, such as phone numbers, would be published. However, since we have DIDs, it is more appropriate to leverage existing protocols for encrypted peer-to-peer communication, i.e., DIDComm. This allows the entire communication during incident response to occur within the scope of the SSI ecosystem. Traditional means should be maintained as a backup.

Further communication with SSI externals must be carried out depending on the SSI system and the incident. For example, to comply with local institutions and laws or to communicate with the media. Internet service providers can be asked for aid to combat large-scale network attacks. Similarly, software vendors or the open-source community have to be kept in the loop to provide patches and updates, among other things. Finally, communication between different domains might be necessary.

7 Evaluation of the security incident response processes for self-sovereign identities

In order to apply the proposed SIR processes, we use the incidents of credential fraud (see Section 7.1), compromised issuer or verifier (see Section 7.2), and attacks on the trust registry (see Section 7.3), as outlined by Naik et al. [5] (see Section 2.3) and introduced in Section 2.3.

7.1 Credential fraud

We assume a scenario in which a verifier becomes aware of malicious activity concerning a credential issued to a holder. This could be the consequence of an attacker stealing a wallet. The attacker tries to utilize the wallet to perform identity transactions, but the verifier notices that the wallet might have been compromised. Consequently, they alert the incident coordinating team, which, in turn, identifies the credentials' issuer and informs them about the fraudulent activities. Since the issuer trusts the incident coordinating team and after performing their own investigation, they update the tails file and publish a new accumulated value on a revocation registry on the blockchain. This tails file is used to revoke credentials without having to utilize an explicit revocation list. As long as the holder can show the verifier that they can use their factor from the tails file, their credentials have not been revoked. When an issuer removes the holder's tails file entry and publishes the new result, the holder cannot provide this proof anymore. As a result, the attacker can no longer use the compromised wallet. Additionally, the issuer notifies as many of the holder's agents as possible. The notification can be conducted directly since the latter has published points of contact. However, the global IRT can step in and contact agents since they have more capabilities. After containing the issue, the issuer, verifier, and IRT can close the incident.

7.2 Compromised issuer or verifier

In this scenario, we assume that an issuer's signing key for credentials and verification key used for authenticating the issuer's DID have been compromised. Compromising both keys allows an attacker to perform two attacks: creating fake credentials signed by a legitimate signing key and spoofing the issuer by crafting a fake DID with a DDO based on the stolen verification key.

Detection of issuer spoofing can originate from multiple sources, such as a verifier noticing a previously unknown second instance of the same issuer. After the issuer discovers the incident, they follow the outlined SIR process. The local IRT starts an internal investigation and the coordination team is informed by submitting an initial report. As a quick containment method, the issuer's stolen verification key is replaced and the DDO is updated. As a corollary, the fake issuer cannot perform writes to the ledger anymore. The global IRT notifies all possible verifiers. Any verifier that wrongfully validated a credential of that issuer is then mandated to access the details of these occurrences while following internal procedures to suspend any service being illegitimately accessed. Next, verifiers inform all owners of fake credentials. Ideally, the affected issuer can identify the source of the incident to eradicate it permanently. Afterward, a full report is submitted to the global IRT.

Possible indicators of a fake credential being created by a legitimate issuer could be a suspicious increase in issuing credentials, other internal security controls being offline, or external parties notifying the issuer. For initial containment, the issuer's signing key is replaced, invalidating all credentials signed with that key. When the exact time of the key compromise becomes clear and the steps that led to the compromise are known, all credentials signed since then are revoked by the issuer. These steps are communicated to the global IRT, which informs the verifiers. Contrary to the first incident, the issuer can inform the holders. The following steps are similar.

For verifiers, we focus on credential creep and background attacks on the verifier, which both target holders' PIIs. Detection could be based on internal monitoring systems, holder complaints, or a drop in user interactions. The SIR process described in Section 6.2 is applied. All affected holders are alerted that their data has been stolen.

7.3 Compromised trust registry

In contrast to the incidents described beforehand, these incidents have been observed in other blockchain applications; see, for example, CVE-2022–31020 [70]. We assume that the underlying trust registry has this vulnerability and that an attacker uses it to attempt to delete the private keys of the node. For this to work, the authentication to access the vulnerable request handlers and the nodes' setup must be improperly configured. The attacker disables all affected nodes by deleting their private keys. Consequently, the network monitoring of the global IRT registers a sudden increase in latency and a decrease in data throughput. This starts the SIR process and an initial assessment is conducted. Further investigation reveals that half of the validator nodes are not participating in the consensus algorithm or writing to the ledger. If a local IRT submits an incident describing the modification of the private key, then the global IRT links both incidents and asks the local IRT for all recent logs of network requests transmitted to the node. Thereby, the global IRT should notice a malicious payload being sent to the vulnerable handler. As a first measure, publicly exposed nodes are isolated by a firewall. Next, a response strategy is designed in which affected node operators are urged to conduct further investigations and rebuild their node with a new private key and a correctly implemented isolation policy. Lastly, the global misconfiguration of the affected request handlers is fixed to authenticate all incoming requests properly. The steps are included in the final report, which is propagated to all node operators in the network.

7.4 Evaluation results

We reconstructed three incidents to evaluate the designed SIR processes. Exemplarily, we described the processes with all involved entities and their roles and responsibilities. Following this, we notice that all designed SIR processes can be applied without any issues or missing steps and, therefore, that they comprise all relevant aspects.

8 Results and discussion

We built a decentralized SIR process for SSI by grouping all relevant actors into three domains according to their goals concerning incident response. Concerning the mediums of communication, we leveraged the communication protocol DIDComm as the primary means to transfer messages within the SSI ecosystem. In doing so, we did recommend templates but did not specify those. This is up for future work. One issue is that holders cannot adequately respond to security incidents. They typically have neither the capabilities nor the tools available. However, since holders typically use wallets to manage their identity data, incident reporting could be introduced to wallets, providing a GUI and pre-filled input. Consequently, more research is required. Controversially, the SIR processes utilize centralized parties, which partly contradicts the core principle of SSI. However, we might need to distinguish between community-driven SSI and SSI for commercial or governmental purposes with higher requirements concerning security. A specific use case could be a centralized SIR process if existing infrastructure is combined with proxies within federations.

The centralized and the decentralized SIR processes have been designed with pre-defined assumptions and conditions. These were stated as broadly as possible to include different use cases and technologies. Nonetheless, they were designed with specific technologies in mind since these were best documented when designing the SIR processes. As SSI is designed with layers similarly to the OSI model, the layers' technology can be changed without influencing the other layers. Therefore, the processes described above apply regardless of the actual deployed SSI technologies. However, as SSI is currently not operated in live operation, practical experiences, which include security incidents and following SIR processes, are missing. Thereby, practically required changes may occur.

The SIR processes have to be evaluated in practice in the future. Another issue is that SSI is not a mature IdM model. Hossain et al. [71] compare SciTokens, VCs, and smart contracts. The authors notice different approaches for revocation, such as using a data registry or new smart contracts. However, Freitag [72] showed that there is no perfect revocation method, as they either have privacy or scalability issues. Hence, the incident shown cannot be solved perfectly; however, with SIR processes, it can at least be solved. Depending on the future development, changes to the processes may be required. When SSI is practically set up, then the processes can be evaluated in practice.

9 Conclusion and outlook

Due to the new eIDAS regulation, elements of SSI are planned to be introduced into today's eID system. However, we found very little literature concerning security or SIR processes for SSI. Consequently, we established a decentralized SIR process for SSI. For this, we evaluated existing approaches for their SIR processes, the challenges they face, and the governance structure and elements of SSI. Based on the analysis, we proposed SIR processes for all three domains. To evaluate our approach, we constructed at least one incident scenario for each domain and applied the proposed SIR processes.

During our analysis, we also noticed that more work is required to enable users to initiate SIR systematically and transparently. Hence, we want to focus on wallet security and design concerning SIR in future work. Additionally, we want to analyze the security threats of SSI in general and specific architectures, such as with OAuth and OIDC. Then, we will apply the results to various use cases, such as the Internet of Things. Finally, we want to evaluate the potential of cyber threat intelligence for SSI.

10 Interview questions used as a guideline

- What is x and what kind of work do you do?
- In this transition from test to productive network, are there any security challenges?
- Are you familiar with any SSI or decentralized identity governance framework or policy concerned with incident response? If not, would such a policy or framework be useful from your perspective?
- How are security incidents meant to be detected, classified, or contained, and who is involved in the decision-making process? Do you provide a framework for incident handling to your members?

Abbreviations

ACApy	Aries Cloud Agent - Python
AD	Active Directory
API	Application programming interface
BISCUIT	Blockchain security incident reporting system based on human observations
DDO	DID document
DeFi	Decentralized finance
DID	Decentralized identifier
DIDAuth	DID authentication
DIDComm	DID communication

DLT	Distributed ledger technology
eduGAIN	EDUcation Global Authentication INfrastructure
eID	electronic identity
eIDAS	electronic Identification, Authentication and Trust Services
FIM	Federated identity management
GDPR	General Data Protection Regulation
GUI	Graphical user interface
IdM	Identity management
IdMS	Identity management system
IRP	Incident response plan
IRT	Incident response team
LDAP	Lightweight directory access protocol
NIST	National Institute of Standards and Technology
NREN	National research and education network
OAuth	Open Authorization
OIDC	OpenID Connect
OSI	Open Systems Interconnection
PII	Personally identifiable information
PKI	Public key infrastructure
REFEDS	Research and Education FEderationS
REST	Representational state transfer
SAML	Security assertion markup language
SIR	Security incident response
Sirtfi	Security incident response trust framework for federated identity
SSI	Self-sovereign identity
SSO	Single sign-on
TLP	Traffic light protocol
TTP	Trusted third party
UMA	User-managed access
URN	Uniform resource name
UUID	Universally unique identifier
VC	Verifiable credential
VON	Verifiable Organizations Network
ZKP	Zero-knowledge proof

Acknowledgements
We would like to thank Soleiman Payman for his input regarding the centralized SIR process.

Authors' contributions
L.Z. analyzed, designed, and implemented SIR for SSI. M.G., D.P., and W.H. validated methodology, architecture, and implementation, and contributed in writing/revising the manuscript. All authors read and approved the final manuscript.

Funding
Open Access funding enabled and organized by Projekt DEAL. This work was partly funded by the University of the Bundeswehr Munich.

Data availability
No datasets were generated or analyzed during the current study.

Declarations

Competing interests
The authors declare no competing interests.

Received: 21 February 2024 Accepted: 20 February 2025
Published online: 20 March 2025

References

1. T. Aditya Sai Srinivas, R. Somula, K. Govinda, in *Smart Intelligent Computing and Applications: Proceedings of the 3rd International Conference on Smart Computing and Informatics, Volume 1, Singapore, Singapore*. Privacy and Security in Aadhaar (Springer, 2020), pp. 405–410
2. P. Singh, Aadhaar and data privacy: biometric identification and anxieties of recognition in India. Inf. Commun. Soc. **24**(7), 978–993 (2021)
3. Dutch National Police Force, *Global police operation: arrests for online identity theft with millions of victims* (2023), www.politie.nl/en/news/2023/april/5/operation-cookiemonster.html. Accessed 20 Dec 2024
4. European Parliament and Council, *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*. Technical report (2014), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. Accessed 20 Dec 2024
5. N. Naik, P. Grace, P. Jenkins, in *Proceedings of the 7th IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 05-07 Dec 2021*. An Attack Tree Based Risk Analysis Method for Investigating Attacks and Facilitating Their Mitigations in Self-Sovereign Identity (IEEE, Piscataway, 2021), pp. 1–8. https://doi.org/10.1109/SSCI50451.2021.9659929
6. N. Naik, P. Grace, P. Jenkins, K. Naik, J. Song, An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. Comp. Secur. **120**, 102808 (2022). https://doi.org/10.1016/j.cose.2022.102808
7. A. Grüner, A. Mühle, N. Lockenvitz, C. Meinel, Analyzing and comparing the security of self-sovereign identity management systems through threat modeling. Int. J. Inf. Secur. (2023). https://doi.org/10.1007/s10207-023-00688-w
8. D. Pöhn, M. Grabatin, W. Hommel, in *Open Identity Summit 2023*. Modeling the Threats to Self-Sovereign Identities (Gesellschaft für Informatik e.V., Bonn, 2023), pp. 85–96. https://doi.org/10.18420/OID2023_07
9. A. Carblanc, in *Identity, security and democracy*. Human rights, identity and anonymity: Digital identity and its management in esociety (IOS Press, Amsterdam, 2009), pp. 11–18
10. H. L'Amrani, B.E. Berroukech, Y. El Bouzekri El Idrissi, R. Ajhoun, in *Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 24-26 Oct 2016*. Identity management systems: Laws of identity for models7 evaluation (IEEE, Piscataway, 2016), pp. 736–740. https://doi.org/10.1109/CIST.2016.7804984
11. J. Sermersheim, *Lightweight Directory Access Protocol (LDAP): The Protocol* (RFC 4511, RFC Editor, Wilmington, 2006), https://www.rfc-editor.org/rfc/rfc4511.txt. Accessed 20 Dec 2024
12. N. Ragouzis, J. Hughes, R. Philpott, E. Maler, *Security Assertion Markup Language (SAML) V2.0 Technical Overview* (Oasis security services technical committee standard, OASIS, Woburn, 2008), https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html. Accessed 20 Dec 2024
13. M.B. Jones, D. Hardt, *The OAuth 2.0 Authorization Framework: Bearer Token Usage* (RFC 6750, RFC Editor, Wilmington, 2012), https://www.rfc-editor.org/rfc/rfc6750.txt. Accessed 20 Dec 2024
14. N. Sakimura, J. Bradley, M.B. Jones, B. de Medeiros, C. Mortimore, *OpenID Connect Core 1.0 incorporating errata set 1* (Standard, OpenID Foundation, San Ramon, 2014), https://openid.net/specs/openid-connect-core-1_0.html. Accessed 20 Dec 2024
15. R. Hedberg, M.B. Jones, A.A. Solberg, J. Bradley, G. De Marco, V. Dzhuvinov, *OpenID Federation 1.0 - draft 36* (Draft, OpenID Foundation, San Ramon, 2024), https://openid.net/specs/openid-federation-1_0.html. Accessed 20 Dec 2024
16. O. Terbu, T. Lodderstedt, K. Yasuda, A. Lemmon, T. Looker, *OpenID Connect for Verifiable Credentials* (Draft, OpenID Foundation, San Ramon, 2022), https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0-ID1.html. Accessed 20 Dec 2024
17. T. Lodderstedt, K. Yasuda, T. Looker, *OpenID for Verifiable Credential Issuance* (Draft, OpenID Foundation, San Ramon, 2022), https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-06.html. Accessed 20 Dec 2024
18. O. Terbu, T. Lodderstedt, K. Yasuda, T. Looker, *OpenID for Verifiable Presentations - draft 20* (Draft, OpenID Foundation, San Ramon, 2023), https://openid.net/specs/openid-4-verifiable-presentations-1_0.html. Accessed 20 Dec 2024
19. K. Yasuda, M.B. Jones, T. Lodderstedt, *Self-Issued OpenID Provider v2 – draft 13* (Standard, OpenID Foundation, San Ramon, 2023), https://openid.net/specs/openid-connect-self-issued-v2-1_0.html. Accessed 20 Dec 2024

20. E. Maler, M. Machulak, J. Richer, *User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization* (Kantara Specification, Kantara Initiative, Herndon, 2018), https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html. Accessed 20 Dec 2024
21. C. Allen, *The Path to Self-Sovereign Identity* (2016), www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/. Accessed 20 Dec 2024
22. M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, C. Allen, *W3C Decentralized Identifiers (DIDs) v1.0* (W3C recommendation, W3C, Cambridge, 2022). https://www.w3.org/TR/did-1.0/. Accessed 20 Dec 2024
23. M. Sporny, D. Longley, D. Chadwick, *Verifiable Credentials Data Model v1.1* (W3C recommendation, W3C, Cambridge, 2022). https://www.w3.org/TR/vc-data-model/. Accessed 20 Dec 2024
24. J. Hasan, Overview and Applications of Zero Knowledge Proof (ZKP). Int. J. Comput. Sci. Netw. **8**, 436–440 (2019)
25. M. Sabadello, *Understanding DID Auth* (2018), www.w3.org/Security/201812-Auth-ID/04_-_Day_1_-_Understanding_DID_Auth.pdf. Accessed 20 Dec 2024
26. Decentralized Identity Foundation, *DIDComm Messaging v2.x Editor's Draft* (2024), www.identity.foundation/didcomm-messaging/spec/. Accessed 20 Dec 2024
27. *Sovrin Glossary V3* (2019), https://docs.google.com/document/d/1gflz5TT0cNp2kxGMLFXr19x1uoZsruUe_0glHst2fZ8. Accessed 20 Dec 2024
28. D. Pöhn, M. Grabatin, W. Hommel, eID and Self-Sovereign Identity Usage: An Overview. Electronics **10**(22), (2021). https://doi.org/10.3390/electronics10222811
29. A. Hedayati, H.A. Hosseini, A Survey on Blockchain: Challenges, Attacks, Security, and Privacy. Int. J. Smart Electr. Eng. **10**(03), 141–168 (2021)
30. M.R. Ahmed, A.M. Islam, S. Shatabda, S. Islam, Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access **10**, 113436–113481 (2022)
31. T. Guggenberger, V. Schlatt, J. Schmid, N. Urbach, in *Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Dubai, UAE, 12-14 July 2021*. A Structured Overview of Attacks on Blockchain Systems. (AIS, London 2021)
32. V. Schlatt, T. Guggenberger, J. Schmid, N. Urbach, Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. Int. J. Inf. Manage. **68**, 102470 (2023)
33. B.G. Kim, Y.S. Cho, S.H. Kim, H. Kim, S.S. Woo, A Security Analysis of Blockchain-based DID Services. IEEE Access **9**, 22894–22913 (2021)
34. F. Schardong, R. Custódio, Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors **22**(15), 5641 (2022)
35. P. Dingle, S. Hammann, D. Hardman, C. Winczewski, S. Smith, *Attempts to Abuse a Verifable Credential* (2019), https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/alice-attempts-abuse-verifiable-credential.pdf. Accessed 20 Dec 2024
36. D. Pöhn, M. Grabatin, W. Hommel, Analyzing the Threats to Blockchain-Based Self-Sovereign Identities by Conducting a Literature Survey. Appl. Sci. **14**(1), (2024). https://doi.org/10.3390/app14010139
37. P. Cichonski, T. Millar, T. Grance, K. Scarfone, *NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology* (Technical report, National Institute of Standards and Technology, Gaithersburg, 2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Accessed 20 Dec 2024
38. ISO, *Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management* (Standard, International Organization for Standardization, Geneva, 2016)
39. P. Cichonski, T. Millar, T. Grance, K. Scarfone, *NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide* (Special publication, National Institute of Standards and Technology, 2012). https://doi.org/10.6028/NIST.SP.800-61r2
40. ENISA, *Good practice guide for incident management* (2010), www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. Accessed 20 Dec 2024
41. D. Schlette, M. Caselli, G. Pernul, A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. IEEE Commun. Surv. Tutorials **23**(4), 2525–2556 (2021). https://doi.org/10.1109/COMST.2021.3117338
42. M. Ioannou, E. Stavrou, M. Bada, in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination (2019), pp. 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885240
43. E.M. Redmiles, in *2019 IEEE Symposium on Security and Privacy (SP)*. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response (2019), pp. 920–934. https://doi.org/10.1109/SP.2019.00059
44. REFEDS, *A Security Incident Response Trust Framework for Federated Identity (Sirtfi) Version 2* (Framework, REFEDS, Cambridge, 2022). www.refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf. Accessed 20 Dec 2024
45. REFEDS, *Refeds - About* (2024), www.refeds.org. Accessed 20 Dec 2024
46. R. Graf, R. King, in *Proceedings of the 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 29 May - 01 June 2018, Piscataway, NJ, USA*. Neural Network and Blockchain Based Technique for Cyber Threat Intelligence and Situational Awareness (IEEE, 2018), pp. 409–426
47. A. Adebayo, D.B. Rawat, L. Njilla, C.A. Kamhoua, *Blockchain-enabled Information Sharing Framework for Cybersecurity* (Wiley, New York, 2019), pp. 143–158. https://doi.org/10.1002/9781119519621.ch7
48. F. Reid, M. Harrigan, in *Security and privacy in social networks*. An Analysis of Anonymity in the Bitcoin System (Springer, New York, 2013), pp. 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10
49. C. Rondanini, B. Carminati, F. Daidone, E. Ferrari, in *Proceedings of the 17th IEEE International Conference on Services Computing (SCC), Beijing, China, 07-11 Nov 2020*. Blockchain-based controlled information sharing in inter-organizational workflows (IEEE, Piscataway, 2020), pp. 378–385. https://doi.org/10.1109/SCC49832.2020.00056
50. B. Carminati, C. Rondanini, E. Ferrari, in *Proceedings of the 25th IEEE International Conference on Web Services (ICWS), San Francisco, CA, USA, 02-07 July 2018*. Confidential Business Process Execution on Blockchain (IEEE, Piscataway, 2018), pp. 58–65. https://doi.org/10.1109/ICWS.2018.00015
51. C.A. Ardagna, M. Anisetti, B. Carminati, E. Damiani, E. Ferrari, C. Rondanini, in *Proceedings of the 17th IEEE International Conference on Services Computing (SCC), Beijing, China, 07-11 Nov 2020*. A Blockchain-based Trustworthy Certification Process for Composite Services (IEEE, Piscataway, 2020), pp. 422–429. https://doi.org/10.1109/SCC49832.2020.00062
52. A. Michail, *Tackling the Challenges of Information Security Incident Reporting: A Decentralized Approach* (Ph.D. thesis, University of East London, 2020)
53. B. Putz, M. Vielberth, G. Pernul, in *Proceedings of the 17th ACM International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 24-26 Aug 2022*. BISCUIT- Blockchain Security Incident Reporting based on Human Observations (Association for Computing Machinery, New York, 2022), pp. 1–6
54. D. Reed, J. Law, D. Hardman, *The Technical Foundations of Sovrin, A White Paper from the Sovrin Foundation* (Whitepaper, Sovrin Foundation, 2016). https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf. Accessed 20 Dec 2024
55. Sovrin Foundation, *Transaction Endorser Technical and Organizational Policies V1* (2019), https://sovrin.org/wp-content/uploads/Transaction-Endorser-Technical-and-Organizational-Policies-V1.pdf. Accessed 20 Dec 2024
56. Sovrin Foundation, *Steward Technical and Organizational Policies V3* (2023), https://drive.google.com/file/d/16Fh423ZqRaUVBjgOsVRXk0VOUUKrYv-p/view. Accessed 20 Dec 2024
57. Ping Identity, *About ShoCard* (2020), www.shocard.com. Accessed 20 Dec 2024
58. uPort, *uPort has evolved* (2021), www.uport.me. Accessed 20 Dec 2024
59. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Technical report, Bitcoin, 2008). Accessed 20 Dec 2024
60. Ethereum Foundation, *Welcome to Etherum* (2024), https://ethereum.org/en/. Accessed 20 Dec 2024
61. Lissi GmbH, *IDunion – An ecosystem for trusted identities* (2024), https://idunion.org/?lang=en. Accessed 20 Dec 2024
62. TNO, *Self-sovereign identity: a simple and safe digital life* (2024), www.tno.nl/en/technology-science/technologies/self-sovereign-identity/. Accessed 20 Dec 2024
63. M. Ma, *EGI.eu Security Incident Response Procedure* (Procedure, EGI, Amsterdam, 2011). Accessed 20 Dec 2024
64. Cybersecurity and Infrastructure Security Agency, *Traffic Light Protocol (TLP) Definitions and Usage* (2022), https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage. Accessed 20 Dec 2024
65. DFN, *Security Incident Response in der DFN-AAI* (2024), www.doku.tid.dfn.de/de:aai:incidentresponse. Accessed 20 Dec 2024

66. ISO, *Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 1: Generic system architectures of mobile eID systems* (Standard, International Organization for Standardization, Geneva, 2023)
67. European Commission, *The European Digital Identity Wallet Architecture and Reference Framework* (2023), https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework. Accessed 20 Dec 2024
68. O. Steeleand, M. Johnson, G. Dardelet, M. Prorock, S. Shetty, D. Kim Hamilton, *Universal Wallet 2020* (Experimental specification, W3C, Cambridge, 2024). https://w3c-ccg.github.io/universal-wallet-interop-spec/. Accessed 20 Dec 2024
69. A. Khayretdinova, M. Kubach, R. Sellung, H. Roßnagel, in *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*. Conducting a Usability Evaluation of Decentralized Identity Management Solutions (Springer Fachmedien Wiesbaden, Wiesbaden, 2022), pp. 389–406
70. NIST, *CVE-2022-31020* (2022), www.nvd.nist.gov/vuln/detail/CVE-2022-31020. Accessed 20 Dec 2024
71. M.J. Hossain Faruk, B. Saha, J. Basney, in *Proceedings of the 7th Practice and Experience in Advanced Research Computing (PEARC), Portland, OR, USA, 23-27 July 2023*. A Comparative Analysis Between SciTokens, Verifiable Credentials, and Smart Contracts: Novel Approaches for Authentication and Secure Access to Scientific Data (Association for Computing Machinery, New York, 2023), pp. 302–305. https://doi.org/10.1145/3569951.3597566
72. A. Freitag, *A new Privacy Preserving and Scalable Revocation Method for Self Sovereign Identity – The Perfect Revocation Method does not exist yet* (Cryptology ePrint Archive, Paper 2022/1658, 2022) https://eprint.iacr.org/2022/1658. Accessed 20 Dec 2024

Publisher's Note