applied sciences

MDPI

Article

An SSI-Based Solution to Support Lawful Interception

Francesco Buccafurri [1], Aurelio Loris Canino [1], Vincenzo De Angelis [2], Annunziata Laurenda [1] and Gianluca Lax [1,*]

[1] DIIES Department, University Mediterranea of Reggio Calabria, 89124 Reggio Calabria, Italy; bucca@unirc.it (F.B.); aurelio.canino@unirc.it (A.L.C.); annunziata.laurenda@unirc.it (A.L.)
[2] DIMES Department, University of Calabria, 87036 Arcavacata di Rende, Italy; vincenzo.deangelis@dimes.unical.it
* Correspondence: lax@unirc.it

Abstract: Lawful Interception refers to the acquisition of the contents of communications between private individuals or organizations by subjects authorized by law. It involves three actors: the network operator (NO), the Law Enforcement Agency (LEA), and the Law Enforcement Monitoring Facility (LEMF). In the literature, standards and scientific solutions are proposed for the interception procedure and the interaction between the NO and the LEMF. However, no standard has been proposed for the interaction between the LEMF and the LEA. The absence of standards for controlling LEA (or a delegated agency) access to intercepted contents stored by the LEMF is a significant gap that should be overcome. This prevents the implementation of secure, interoperable, and automated procedures, leading to inefficiencies and security risks. In this paper, we propose to cover the above gap by adopting the Self-Sovereign Identity (SSI) paradigm. The adopted research methodology follows a multi-phase approach that includes studying existing solutions, system design, and technical feasibility testing. The study first examines existing standards and identity management frameworks and their limitations. Next, an SSI-based architecture is proposed to manage the interactions between LEA (or a delegated agency) and LEMF. Finally, a proof of concept of the proposed solution written in Python and using the Hyperledger Indy blockchain has been implemented to assess whether our proposal is technically feasible. The proposed solution enhances automation, security, and interoperability in lawful interception. Indeed, it enables machine-readable authorizations, reducing errors and improving efficiency by eliminating manual operations. Additionally, verifiable credentials and decentralized identifiers strengthen security and standardize interactions across jurisdictions, ensuring privacy-preserving identity management. By standardizing interactions between LEA and LEMF, this research contributes to a more secure, privacy-preserving, and legally compliant lawful interception process.

Keywords: Self-Sovereign Identity; Sovrin; access control; ETSI; Hyperledge; Trinsic

Academic Editor: David Megías

Received: 20 January 2025
Revised: 9 February 2025
Accepted: 17 February 2025
Published: 19 February 2025

Citation: Buccafurri, F.; Canino, A.L.; De Angelis, V.; Laurenda, A.; Lax, G. An SSI-Based Solution to Support Lawful Interception. *Appl. Sci.* **2025**, *15*, 2206. https://doi.org/10.3390/app15042206

1. Introduction

Lawful interception (LI) is a procedure in which the content of communications among private individuals or organizations is collected and provided to agents authorized by the law [1]. Besides ethical and legal issues [2,3], which are outside the scope of this paper, researchers focused their attention on the technical aspects of the LI procedure.

An LI procedure involves three actors: the Network Operator (NO), which physically intercepts data; the Law Enforcement Monitoring Facility (LEMF), which collects, stores, and analyzes these data; the Law Enforcement Agency (LEA), which accesses the data kept by the LEMF for legal purposes.

The literature includes several proposals and standards regarding both the physical interception of data performed by the NO [4–6] and the provision of these data to the LEMF, such as CALEA [7], 3GPP TS 33.108 [8], ITU-T Y.2770 [9]. Among them, ETSI TS 101 671 V3.15.1, published in June 2018, is the most recent and used technical standard in LI [10]. It has been developed by the European Telecommunications Standards Institute and provides guidelines for implementing the interfaces and processes required for LI, ensuring compliance with legal and regulatory frameworks while maintaining the integrity and privacy of intercepted data. Three Handover interfaces are defined to govern communication between the NO and the LEMF. Moreover, data types specifying the handling of intercepted information as well as mechanisms to ensure the confidentiality and integrity of intercepted data are defined. ETSI TS 101 671 serves as a foundational framework for lawful interception across jurisdictions, promoting interoperability and standardization while addressing privacy and ethical considerations.

However, to the best of our knowledge, the interaction between the LEMF and the LEA is not explicitly addressed in ETSI TS 101 671 or other standards. This leads to the adoption of different practices across countries [11,12], mostly based on manual, non-secure processes, which can cause security and efficiency concerns, including increased risks of errors, delays, and data integrity violations. This issue becomes even more critical in cross-border investigations, where the LEA may delegate access to intercepted data to an External Agency (EA). Without standardized authentication and authorization mechanisms, an EA can retain access beyond the authorized period or an insider within the agency could extract sensitive information without detection. These vulnerabilities expose lawful interception systems to potential data leaks, unauthorized disclosures, and operational inefficiencies.

In this paper, we aim to cover the above gap by adopting the Self-Sovereign Identity (SSI) paradigm [13–16]. SSI is a new paradigm that empowers people to own and control their data without relying on centralized entities. SSI provides several advantages over alternative approaches such as federated identity management (FIM) and authentication based on Public Key Infrastructure (PKI). Unlike FIM, which relies on trusted third parties (e.g., Google or Facebook) to authenticate users, or PKI-based solutions, which require certificate authorities to manage certificates, SSI is a decentralized approach that eliminates bottlenecks and single points of failure. The privacy-preserving nature of SSI allows users to selectively disclose only the necessary information without revealing their full identity. This is in accordance with the minimization principle of GDPR. In contrast, FIM and PKI solutions require continuous involvement of identity providers, and privacy concerns may arise from honest but curious providers that legitimately participate in the users' authentications but also have the ability to infer sensitive information from the observed user behaviors. Another advantage of SSI is its interoperability and portability. PKI requires multiple certificates for different services, and FIM systems need pre-established agreements between providers, limiting their portability. In contrast, verifiable credentials are used in SSI that can be interoperable across different organizations and jurisdictions (even if this introduces trust problems in cross-border authentication that should be suitably addressed in each specific application context). Overall, the numerous advantages of SSI make it the preferred solution for the future of digital identity [17].

For these reasons, we propose a solution relying on the state-of-the-art SSI Sovrin framework [18]. A core element of our proposal is the access control mechanism built on top of the SSI substrate. This aspect is very relevant, especially in the case of the LEA relying on an external agency to collect such data. In this case, proper authorizations should be provided to prevent unauthorized access. Although some guidelines are provided in this direction (such as the adoption of RBAC [19] or VACM [20]), no concrete proposal is currently available.

Another relevant aspect of our contribution is that the proposed solution applies to real-life contexts. Indeed, it is compliant with the Sovrin SSI stack [21,22] and its evolution, the ToIP stack [23]. The above framework represents the state of the art in the SSI environment [24]. Starting from this framework, we built a proof of concept of the solution (publicly available on GitHub) using standard and well-consolidated technologies. We used this proof of concept to verify that the designed solution is technically possible. However, the used code has been developed quickly and lacks scalability, security, and integration with existing infrastructure, thus making it unsuitable for real-world experimentation.

The proposed solution provides three key benefits related to automation, security, and interoperability in lawful interception procedures, which are discussed below. Unlike traditional lawful interception, which is usually handled by manual operations, our solution enables machine-readable authorizations, allowing access control, credential issuance, and verification to be fully automated. In this way, the absence of human intervention minimizes errors and improves efficiency. The use of verifiable credentials enhances security by eliminating the need for centralized identity providers, which can be hacked or manipulated, reducing single points of failure. Moreover, selective disclosure is supported, allowing users to share only necessary information and thus reducing privacy concerns. The lack of standardized interaction protocols between LEA and LEMF has led to fragmented implementations across different countries. Our solution addresses this problem using decentralized identifiers, Verifiable Credentials that follow the W3C format, and the DIDComm protocol, which ensures that different entities involved in the LI procedure, even across various jurisdictions and countries, can seamlessly interact.

This paper is structured as follows. In the next section, we provide background notions about the LI procedure and the SSI paradigm. In Section 3, we discuss the faced problem and highlight the contribution of the proposed solution. The proposed approach is described in Section 4. In Section 5, we design the SSI stack underlying our approach and, in Section 6, we provide a proof of concept. The related literature is contextualized in Section 7. Finally, in Section 8, we draw our conclusion.

2. Background

This section presents the concepts of LI and SSI, which will be widely used in the following.

2.1. Lawful Interception

Lawful interception is a procedure in which a network operator provides a law enforcement agency with intercepted communications of individuals. In the following, we refer to the standard ETSI TS 101 671 V3.15.1 [10] adopted in many countries: anyway, the results emerging from this research apply also when considering other standards such as CALEA [7] (adopted in the U.S.) or 3GPP TS 33.108 [8] (used for mobile networks).

The LI procedure involves three actors: the LEA, the LEMF, and the NO.

- The LEA is the Law Enforcement Agency that is involved in a certain investigation about one or more individuals;
- The LEMF (Law Enforcement Monitoring Facility) is the transmission destination for the results of interception;
- The NO is the telecommunication operator offering the network platform to the individuals under investigation.

LI deals with two types of data: Intercepted Related Information (IRI) and Content of Communications (CC). IRI refers to the metadata of the communications, such as the source and destination of a call, whereas CC refers to the real content of the communications (video, messages, and so on). According to [10], in a LI procedure, there are three logical

interfaces used for the communication between the actors, called handover interfaces, which are HI1, HI2, and HI3. The HI1 interface is used between the LEA and the NO to exchange useful information about the activation and deactivation of the LI procedure regarding a certain target. The HI2 interface is used for the transport of the IRI from the NO to the LEMF. The H13 interface is used for the transport of the CC from the NO to the LEMF.

We conclude this section by observing that there is no standard interface or protocol to handle communication between LEA and LEMF. This observation represents the starting point of our study.

2.2. Self-Sovereign Identity

Self-Sovereign Identity (SSI) offers a new way to manage digital identities based on decentralization. The main innovation of this paradigm is that the locus of control shifts to the owner of an identity (e.g., person, animal, organization, or object) who can interact with everyone else as a full peer. SSI can be defined as a set of technologies that are put together to create a new model for digital identity management. In this section, we discuss the most relevant features of each building block of SSI that have been used in our proposal.

2.2.1. Verifiable Credentials

The Verifiable Credential (VC) is a set of information that some authority claims to be true about a specific entity that is the subject of the credential. In SSI, the authority is called issuer, while the subject of the VC is called holder. The holder can prove something about themselves by presenting their VC to a verifier. At a high level, the structure of the VC includes four sections:

- Identifier of the VC;
- VC metadata (e.g., issue date, expiration date, state of the credential);
- VC's claims about the subject;
- Proof, which is the digital signature of the issuer of the credential. It can be verified through the blockchain.

2.2.2. Issuers, Holders, and Verifiers

Issuers, holders, and verifiers are the three roles involved in the SSI system, also known as the Trust Triangle. The issuers are the source of VCs, and they are usually some authorities such as universities or companies. The holders are the subjects of the credential that are responsible for storing the VCs in a digital wallet. The holders can be individuals but also organizations or objects. Lastly, the verifiers are the entities that offer a benefit to the holder after the execution of a verification process of one or more credentials. The verifiers can be individuals or organizations. The three actors are involved in several interactions as request, issuing, and verification of the VCs. One of the most relevant interactions between SSI roles is the verification of one or more VCs presented by the holder to the verifier. The verifier must define an access control policy for each benefit they offer. In the SSI world, this policy can be seen as the set of VCs that the holder must present to obtain access to the service. After the presentation process, the verifier starts the verification, which is the union of several steps:

- VC's state verification: the verifier must check that the VC is still valid so that it has not been revoked.
- VC's claims verification: the verifier must check that the information contained in the VC satisfies the access control policy.

- VC's issuer verification: the verifier must check the authenticity of the VC's issuer. The VC includes the issuer's Decentralized Identifier (DID), allowing the verifier to retrieve the issuer's public key from the blockchain to validate the VC's digital signature.

2.2.3. Digital Wallet

The digital wallet is the location where the VCs are stored securely. It is a software application installed in a generic device such as a smartphone, tablet, or laptop. The owner of the digital wallet is the holder of the VCs. Strong authentication processes must be implemented to access the wallet because it contains private and sensible information. The digital wallet is configured to maintain:

- Verifiable Credentials (VCs) issued to the holder of the digital wallet
- Peer Decentralized Identifiers (Peer DIDs) used to establish the peer-to-peer connections

2.2.4. Digital Agents

The Digital Agent is a software module that helps the user during the interactions with their digital wallet. The digital agent executes several actions on behalf of the owner of the wallet. As an example, the digital agent generates a new peer DID when the owner wants to establish a new peer-to-peer connection, or it stores the VCs in the wallet when the owner accepts it.

The peer-to-peer connections, which have been mentioned above, are widely used in our proposal. A peer-to-peer connection is established off-chain after some actions are taken by the controller (owner of the wallet) as a QRCode scan or a click of a link. If the controller authorizes the connections, the digital agent will prepare all the cryptographic materials necessary to establish the connection. On these connections, the VCs can be exchanged between the holder, issuers, and verifiers.

2.2.5. Decentralized Identifies

Decentralized Identifiers (DIDs) are a type of URI that uniquely identifies an entity in the SSI system. Each DID resolves to a DID Document, which includes details about the identified entity (e.g., the public key for the digital signature verification).

There are two types of DIDs:

- Ledger-based DIDs: this type of DID involves a blockchain or a generic distributed ledger. It is typically the blockchain address. It is created, updated, and deactivated by performing a transaction.
- Peer-DID: this type of DID does not involve a blockchain. Each endpoint of a peer-to-peer connection generates a Peer DID that is securely shared with the other peer entity using a specific communication protocol.

2.2.6. Verifiable Data Registry

A Verifiable Data Registry is used in SSI to obtain the property of decentralization to create an identity system that supports privacy without a central authority. The verifiable data registry is typically a blockchain used to manage the DIDs and the public keys. The blockchain must be public [25] to enable access to everyone and can be permissioned or permissionless. In our proposal, the blockchain used is Sovrin, which is public and permissioned. It is important to store the DID of the issuers on the blockchain to facilitate the verification process carried out by the verifiers.

2.2.7. Governance Framework

The Governance Framework is the last block of the SSI architecture and involves social and human aspects. Indeed, the Governance Framework simplifies the job of the verifier. A

governance authority publishes a list of trusted issuers. When a verifier receives a new VC issued by a certain authority, they can check the presence of that issuer in the list. If they are present, then they are trusted.

3. Motivations and Goals

The literature includes several proposals for standardizing the interceptions between the NO and the LEA, as well as between the NO and the LEMF, such as CALEA [7], 3GPP TS 33.108 [8], ITU-T Y.2770 [9], and ETSI TS 101 671 V3.15.1 [10]. Among them, the latter is the most recent and used one in LI. However, to the best of our knowledge, the interaction between the LEMF and the LEA is not explicitly addressed in ETSI TS 101 671 or other standards, and the lack of a structured framework for LEA-LEFM interactions introduces three main issues:

1. Interoperability issues: The absence of interoperability standards led each country to adopt and implement its own national procedure to manage the interaction regarding how LEA should retrieve data from LEMF [12]. These methods are often incompatible with each other. This limitation becomes particularly critical in cross-border investigations, where an LEA may need to delegate interception access to an external agency. For example, consider a scenario where an EU member state is investigating a transnational criminal group. The national LEA may require assistance in accessing intercepted communications related to the group's activities. In this case, the LEA can request support from an external agency, such as the NSA, which is the U.S. government agency responsible for foreign and domestic intelligence and counterintelligence purposes. This agency can facilitate access to the necessary data from LEMFs in other states. In this case, proper authorizations should be granted by the LEA to the external agency ensuring that the data are handled in accordance with legal requirements.
2. Procedural inefficiencies: Many lawful interception processes continue to rely on manual and insecure procedures, such as paper-based approvals and email exchanges. These mechanisms could result in operational inefficiencies and human errors and may introduce delays in investigations in which rapid access to the intercepted information is crucial.
3. Security risks: Security risks may arise due to the absence of standardized access control mechanisms. Without a protocol for managing and verifying access to intercepted data, there is no robust way to ensure that only authorized entities retrieve sensitive information. This exposes LI systems to several vulnerabilities, including unauthorized data retention, insider threats, and data leaks. Additionally, the lack of real-time access revocation mechanisms means that once an external agency is granted access to LI data, it may retain that access indefinitely, even after the investigation has concluded, increasing the risk of unauthorized disclosures and violations.

To address these challenges, we propose a decentralized and verifiable credential system based on the SSI paradigm. Our solution ensures that only authenticated and authorized entities can retrieve intercepted data while enabling real-time revocation of access rights to prevent misuse. Our solution provides the following outcomes:

- Fine-tuning: The agency obtains a credential for access to data specific to a certain request, including a validity period to verify whether the authorization has expired;
- Minimality: Data accessed by the agency is selectively disclosed, supporting the principle of minimal information disclosure;

- Revocation: Authorizations can be revoked by the issuer at any time, a significant advantage over standard signature-based solutions where only certificates can be revoked, not specific signatures;
- Automation: Authorizations are machine-readable, enabling fully automated authorization processes;
- Effectiveness: We provide a proof of concept based on established SSI standards, such as the Sovrin framework.

To better understand the points above, we anticipate some details of the solution.

The LEA can play the role of the issuer and release some credentials (i.e., authorizations) to the agency. On the other hand, the LEMF can play the role of the verifier and check the credentials presented by the agency. However, the scenario presented above represents a simplification of a real-life LI procedure. Indeed, when an employee of the agency asks the LEA for the credentials, the LEA has to be sure that such an employee has the right to obtain such credentials. Again, the SSI approach can solve the problem. Indeed, the right to obtain the credentials from the LEA can be granted if the employee provides the LEA with other credentials released by the agency. These new credentials attest that the employee is authorized by the agency to participate in this LI procedure. In other words, in this case, the roles of the parties are different in contrast with the previous case (the agency represents the issuer and the LEA represents the verifier).

In our solution, we pursue the following goals:

- To allow the LEA to start a new LI procedure by commissioning an entity for the role of LEMF. In this phase, the LEA also interacts with the NO according to the standard [10].
- To allow an employee of an external agency to obtain from the LEA the credentials to access an interception procedure already started on the LEMF.
- To allow the LEA to revoke the credentials released to the employee and the LEMF.

The design of the proposed solution is the objective of Section 4.

4. Proposed Approach

The scenario considered in this paper involves five actors. The first three actors have been already presented in Section 2.1 and are the LEA, the LEMF, and the NO. The other two actors are the external agency (EA), which the LEA relies on to access the interception data, and an employee (E) of the EA.

In the following subsections, we define the three phases defined in the proposed solution. In Section 4.1, we present the setup phase, which involves LEA, LEMF, and NO. Although this phase is discussed in [10], some details are neglected, especially with regard to the communication between the LEA and the LEMF. This phase can take advantage of the integration of the SSI approach. Once the LI procedure is started on the LEMF, the LEA charges the EA to access the interception procedure on the LEMF. This task is performed by the employer E properly authorized. This phase is described in Section 4.2. Finally, we present in Section 4.3 the mechanism for revocation, which is run when the interception procedure is complete or when the access needs to be restricted under any other circumstances.

4.1. Setup

Through this phase, the LEA starts a new LI procedure by leveraging the SSI framework. This phase is performed through the following steps:

1. First, the LEA contacts the LEMF to establish a secure peer-to-peer channel according to the DIDComm protocol (see Section 2.2).

2. In this connection, the LEMF provides the LEA with all the technical information needed for the interception procedure (for example, the phone number and the IMEI of the SIM of the intercepted subject).
3. The LEA releases the credential VC_{LEMF} to the LEMF certifying that the latter is in charge of this LI procedure. This credential will be presented by the LEMF in all the next interactions with LEA.
4. Finally, an interaction according to the standard [10] is performed between LEA and the NO, so that the latter can define the interfaces to be used in the interception process.

The above steps are summarized in the sequence diagram of Figure 1.

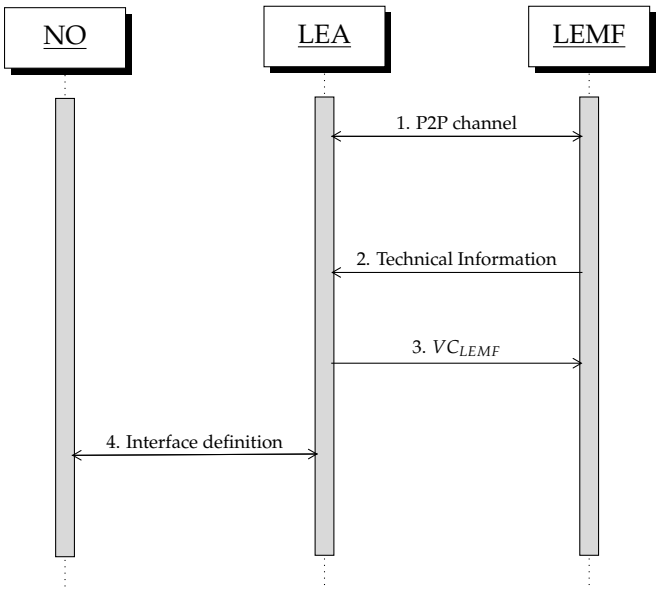


Figure 1. Sequence diagram of the Setup in the LI procedure.

4.2. External Agency Integration

Consider the employee E of the EA authorized by the LEA to access the data related to the LI procedure on the LEMF. We assume that E is preliminarily equipped with a credential VC_E, certifying their identity and role within the EA.

To allow E to access the data on the LEMF, the following steps are performed.

1. Through a secure peer-to-peer channel, E sends the credential VC_E to the EA.
2. The EA verifies VC_E (as described in Section 2.2) and sends to E a new credential VC_L certifying E is authorized by EA to interview in the LI procedure.
3. Through a secure peer-to-peer channel, E sends VC_L to the LEA.
4. The LEA verifies VC_L and grants a new credential VC_{LM} to E. This new credential is used by E to obtain access to the LEMF.
5. Now, through a secure peer-to-peer channel, E sends the credential VC_{LM} to the LEMF.
6. The LEMF verifies this credential (*Check* VC_{LM}) to ensure that it is valid (not expired or revoked), issued by the LEA (checking the digital signature of the credential), and its claims satisfy the access control policy. Whether all these checks are successful, the LEMF grants E access to the interception data by a procedure they agree on (typically, data are sent via a secure channel or a storage device).

The above steps are summarized by the sequence diagram in Figure 2.

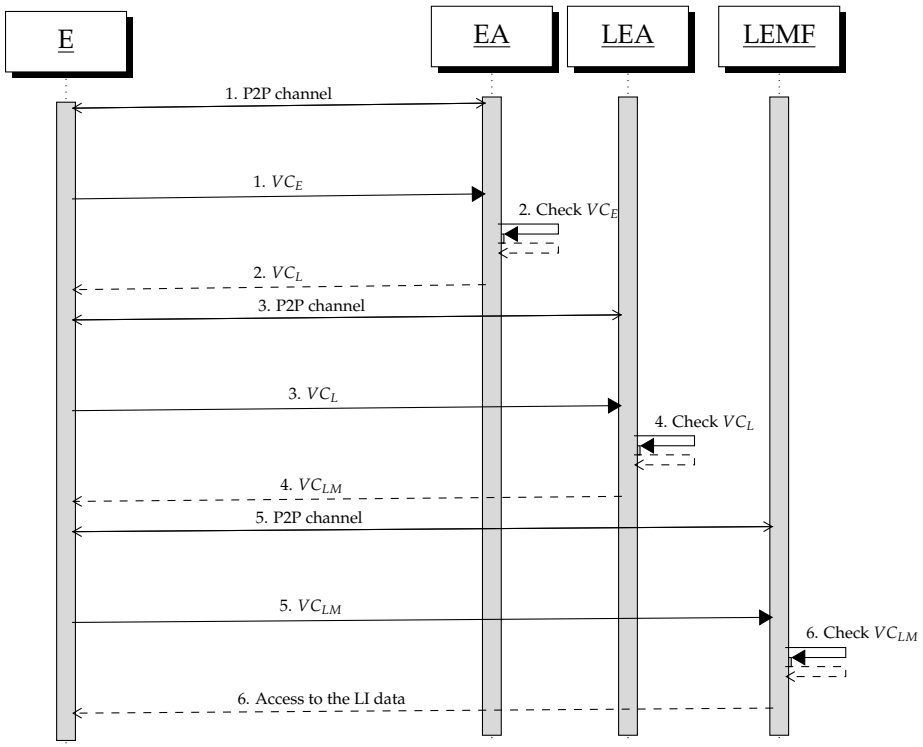


Figure 2. Sequence diagram of the EA integration in the LI procedure.

4.3. Credential Revocation

The duration of an interception procedure is influenced by several factors, mainly the complexity of the case, and predicting how long the procedure should take is not easy. When an expiration time for the verifiable credentials cannot be established, credential revocation should be used. The revocation process occurs after the LI procedure is complete or when the access needs to be restricted under any other circumstances to prevent unauthorized access to entities previously authorized.

Revocation can be triggered by both the LEA and the EA. In the first case, the LEA may revoke both the credential VC_{LEMF} and the credential VC_{LM} to remove the participation of the LEMF and E in the LI procedure, respectively. In the second case, the EA can revoke (i) the credential VC_L or (ii) the credential VC_E. In case (i), the EA removes the participation of E in the LI procedure. Case (ii) happens when E is fired, resigns, or changes role in the agency EA.

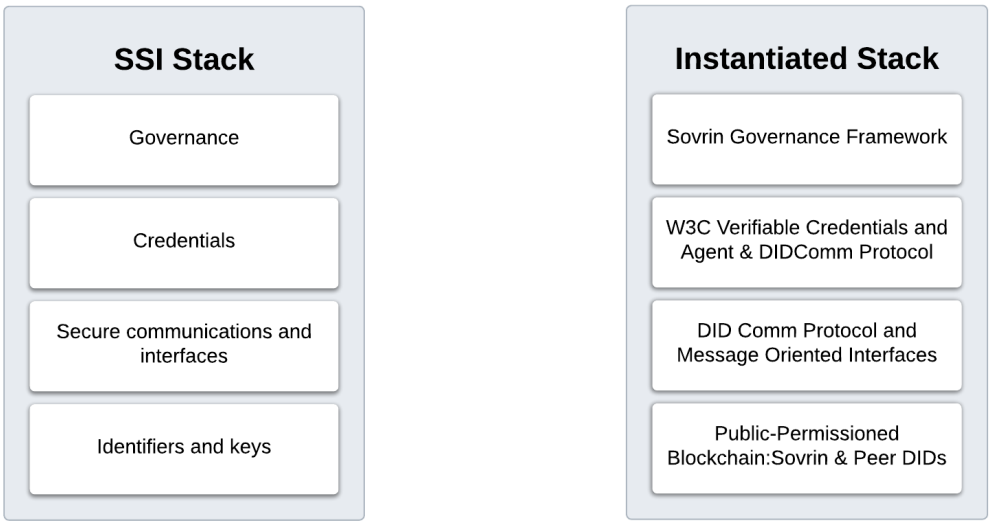
The LEA and EA use the same procedure for revoking credentials, which is based on cryptographic accumulators [26]. A cryptographic accumulator is a data structure that allows the compact representation of a set of elements, enabling efficient membership verification. Given a set of elements, the accumulator produces a concise value that encapsulates all the elements. This structure provides two properties:

1. Membership Proofs: It can be demonstrated that a specific element belongs to the set without revealing other elements of the set.
2. Dynamic Updates: Elements can be efficiently added to or removed from the set.

Each revoked credential becomes part of the revoked credentials set, which updates with each new revocation. Verifying the state of the VC corresponds to verifying the membership of that VC to the set. If the result of the membership of a VC is true, then the verification fails. Using a cryptographic accumulator, our solution provides a secure and decentralized method to manage credential revocations while maintaining the privacy and efficiency required for LI procedures.

5. Design of the SSI Stack

To design our solution also from a technological point of view, we refer to the SSI stack [21] and its evolution, the ToIP stack [23], depicted in Figure 3a. Therein, four layers are introduced that define how trust is achieved among several participants. In the following subsections, we describe the role of each level and how it is used in our approach. The resulting instantiation of the stack in our proposal is reported in Figure 3b.



(**a**) SSI Stack. (**b**) Instantiated SSI Stack.

Figure 3. Comparison between the general SSI stack (**a**) and its instantiated version (**b**).

5.1. Layer 1

The first layer refers to identifiers and keys. It allows the entities of the system to access (read and/or write) data without relying on a third central authority. This requires introducing a verifiable data ledger, known as theDID Registry.

In our solution, we selected Sovrin [18] as DID Register, a special-purpose blockchain deployed for SSI. It is a public and permissioned blockchain [27] (accessible to all entities but only authorized parties can write data on it). We store the following information on the blockchain:

- Public DIDs of LEA, LEMF, and EA: They are the DIDs of the entities playing the role of issuers and verifiers in our approach. They are used by the employee E to establish an off-chain connection with them. Moreover, the public DIDs allow the parties acting as verifiers (i.e., the LEA, the EA, and the LEMF) to obtain the public keys to check a cryptographic proof of ownership of a credential.
- Schema: It defines the format (in terms of allowed attributes) of the credentials released by the issuers. Observe that it does not contain any personal data about the employee E.
- Credential Definition: It is an instance of the Schema including the public keys allowing the verification of the credentials. Similar to the Schema, the Credential Definition does not include any personal data about E. The inclusion of the Schema and the Credential Definition at the blockchain level makes the credential exchanges fully decentralized enabling a fast release and verification of the credentials from anywhere.
- Revocation Registry: We include two revocation registers, one managed by the LEA and one managed by the EA. Only the issuer (LEA or EA) can update each register, which links to a Credential Definition. The registers are stored on-chain, but, again, they do not contain any personal data about E. As the name suggests, they allow

the LEA and the EA to revoke the credentials released to the employee E and the LEMF. They are based on the cryptographic accumulator described in Section 4.3. The advantage of this approach is that the LEA and EA do not have to maintain a public API for the revocation, but the entities playing the role of verifiers can check the revocation of the credentials in a decentralized way by accessing the blockchain.

- Agent Authorization Policies: This component implements a mechanism of protection in the case the device of E is stolen or lost. In the device used by E, an agent is installed to exchange proofs of the credentials owned by E. In the case this device is stolen or lost, a revocation mechanism is enabled. In particular, when E authorizes a new agent (device), an authorization key is stored in an on-chain registry. This key is used to sign messages exchanged peer-to-peer between E and the other entities. To remove the authorization for an agent, E can delete its key from the register.

It is worth highlighting that the following information is not stored on the blockchain:

- Private DIDs: They are the DIDs of the actors used in the peer-to-peer connection.
- Private Data: They are personal data about the employee E. These data have not been stored even in encrypted form. Indeed, since the data stored on the blockchain are immutable, they could be compromised in the long term.

To conclude, we observe that our solution leverages Peer DIDs to establish peer-to-peer communications. Even though the selection of the communication protocol regards Layer 2 of the stack, the choice to rely on Peer DIDs is performed at Level 1. In this case, the DID Registry is represented by the digital wallets of the entities generating and storing the Peer DIDs.

5.2. Layer 2

Layer 2 refers to the communication protocol between agents and the interfaces available to the developers. As mentioned in the previous section, at this level the peer-to-peer communications between agents are established.

The protocol used in our solution is DIDComm [28], which is fully compliant with the ToIP stack. This protocol is based on message exchange and is independent of the underlying transport protocol. Each agent of the communication is identified through a DID and the communication is encrypted through the public key associated with the DID. Since any transport protocol is allowed, the most common choice falls on HTTP or HTTPS (as in our approach), allowing us to develop a web application based on the request-response paradigm (see Section 6). Therefore, no particular technology of the involved parties is required.

At this level, some message-oriented interfaces for the developers are proposed. In detail, we distinguish two types of nodes: agent and validator. The agent nodes can be hosted everywhere (smartphone, laptop, cloud, and so on). Each agent maintains one or more connections, each one associated with a Peer DID. As already discussed, these connections are used to exchange cryptographic credentials and proofs. The validator nodes allow the agent nodes to interface with the blockchain selected in Layer 1. Specifically, in our approach, the agent nodes rely on the validator nodes to access the public keys associated with the public DIDs of the LEA, LEMF, and EA and/or to write the Schema and the Credential Definition before releasing the credentials (in this case the agent nodes are hosted on the issuers).

5.3. Layer 3

Layer 3 defines the format of the credentials and the way in which they are exchanged. Again, to adhere to the ToIP stack, we select the W3C format, which supports ZKP-oriented credentials [29]. The advantage is that the holder (i.e., the employee E) does not need to

present credentials, but only a cryptographic proof of them. This allows us to reduce the information disclosed by E to the minimum.

5.4. Layer 4

The last layer defines the Governance Framework to offer maximum interoperability between different systems [24]. We rely on the Sovrin Governance Framework [30], which defines legal and commercial rules to which all entities must adhere. Actually, this framework covers aspects regarding all four layers of the stack.

5.5. Stack Overview

This four-layer architecture standardizes interactions between LEA, LEMF, and EA without relying on a centralized authority. Without loss of generality, the EA can authenticate itself through a verifiable credential issued by the LEA, which follows the W3C format of Layer 3 and is released using the DIDComm protocol of Layer 2. Additionally, at Layer 1, the Sovrin blockchain acts as a decentralized registry that keeps track of the credential definitions and revocation statuses. This allows different countries or law enforcement agencies to verify digital credentials independently by checking the blockchain, thus ensuring global interoperability. Finally, the Governance Framework defined in Layer 4 ensures that LEA, LEMF, and EA are compliant with legal and security regulations, especially when working across different countries. When different law enforcement agencies or external agencies from different countries need to share or access intercepted data, they must follow the same legal and security guidelines. For example, in a cross-border cybercrime investigation, a European LEA could gain access to the intercepted data from a U.S.-based LEMF by authenticating itself through a verifiable credential, issued under the W3C standard and verified via blockchain. The U.S.-based LEMF can validate the request without manual verification, ensuring secure and interoperable access. Moreover, the adoption of the SSI stack ensures the interoperability between our system and other SSI systems. In practice, this approach allows us to incorporate the verification and exchange of verifiable credentials from other SSI systems adopting the same standard defined in the stack (e.g., law enforcement badges or digital warrants issued as verifiable credentials) into our access control process.

6. Proof of Concept

Through this section, we describe the proof of concept developed to verify the technical feasibility of our proposal (the source code is available at https://github.com/CyberGoldSun/SSI_LI (accessed on 30 January 2025). The proof of concept consists of three web applications that run the procedures done by the LEA, LEMF, and EA, respectively.

6.1. Technologies

We developed the proof of concept using several technologies. First, we adopt the Sovrin framework, which is based on Hyperledger Indy [31], a public permissioned blockchain. Sovrin defines the rules governing the blockchain (consensus protocol, validator nodes, the format of the DIDs, and so on). Among its components, Sovrin includes the agent nodes hosted by the entities participating in the system that allow the exchange of credentials and DIDs.

The second technology used is Trinsic [32], a platform based on Hyperledger Aries that offers several APIs to build SSI ecosystems. In particular, Trinsic supports the Sovrin-defined format for credentials and DIDs. Specifically, we rely on Trinsic Studio to manage the organizations realizing the credentials (of the LEA, LEMF, and EA) and on the Android mobile app to host such credentials. Finally, the web applications are realized from scratch in Python by using the Flask micro-framework [33].

6.2. Case Study

We show the main functionalities offered by our solution through a case study. In particular, we refer to the EA integration in the LI procedure of Section 4.2, which is the more relevant contribution of this paper. Note that some functionalities (such as the revocation) are not included in this case study but are implemented in the version of the software available on GitHub.

In our case study, we consider an employee Bob of an external agency, called NA, who was charged by the LEA to access data relative to an LI procedure on the LEMF. Initially, the three organizations involved in the system register on the Trinsic Studio platform (see Figure 4).

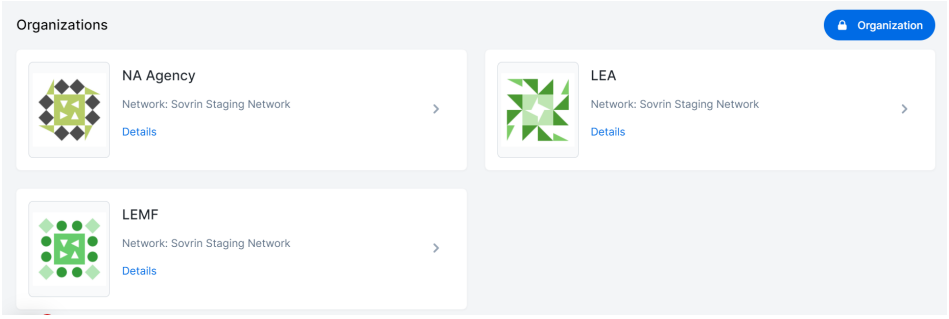


Figure 4. Registration of LEA, LEMF, and NA Agency.

In this registration phase, some fields have to be provided (name, region, blockchain network, and so on). In particular, a relevant field is the issuer DID, which identifies an issuer and is used to verify the credentials it releases. Figure 5 shows an example of the fields associated with the NA agency.

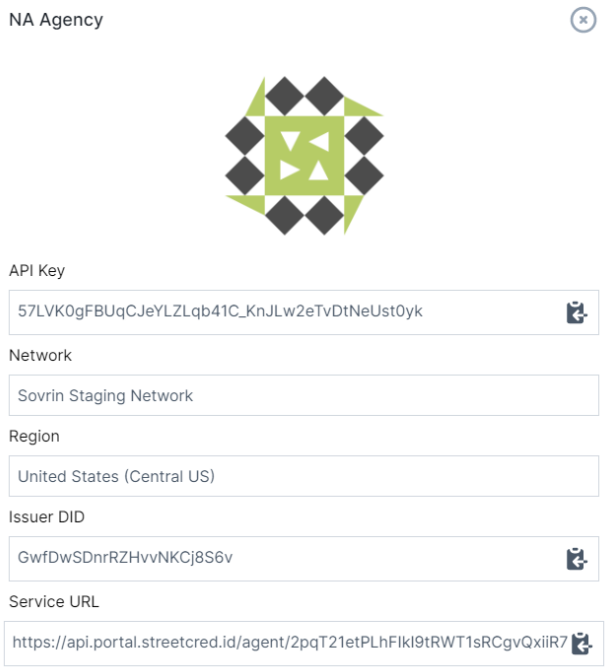
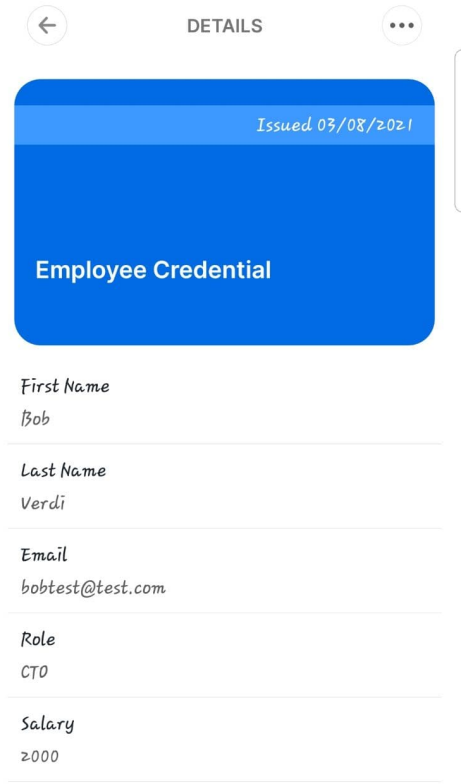
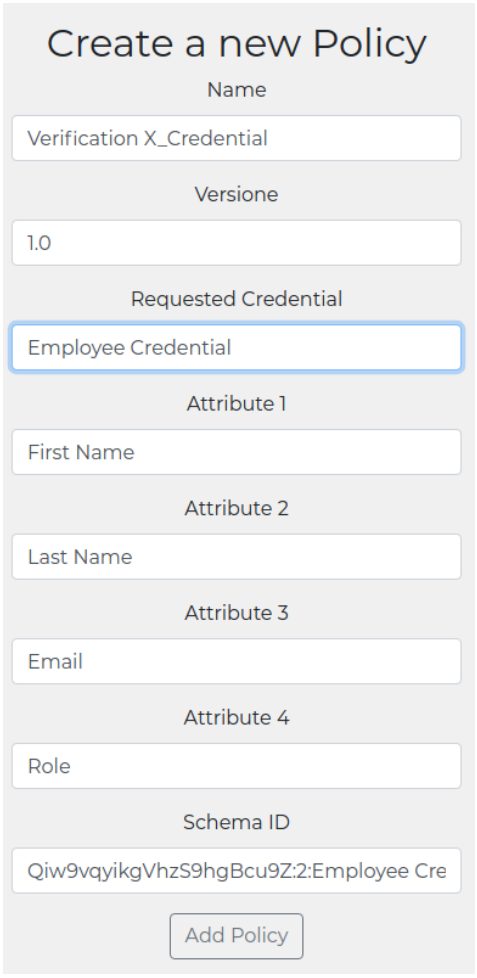


Figure 5. Fields of NA Agency registration.

When Bob is hired by NA, he receives an "Employee credential" certifying its status. This credential (with its fields) is stored on the Bob mobile wallet (Android app) as shown in Figure 6a. To participate in the LI procedure, Bob needs the "X credential" released by the agency NA. As discussed in Section 4.2, to obtain the "X credential", Bob has to prove the ownership of the "Employee credential". The agency NA (through the web application) generates a "Verification" of the "employee credential". This is reported in Figure 6b. Observe that optional attributes may be requested to Bob.



(**a**) Employee Credential.



(**b**) X Credential Verification.

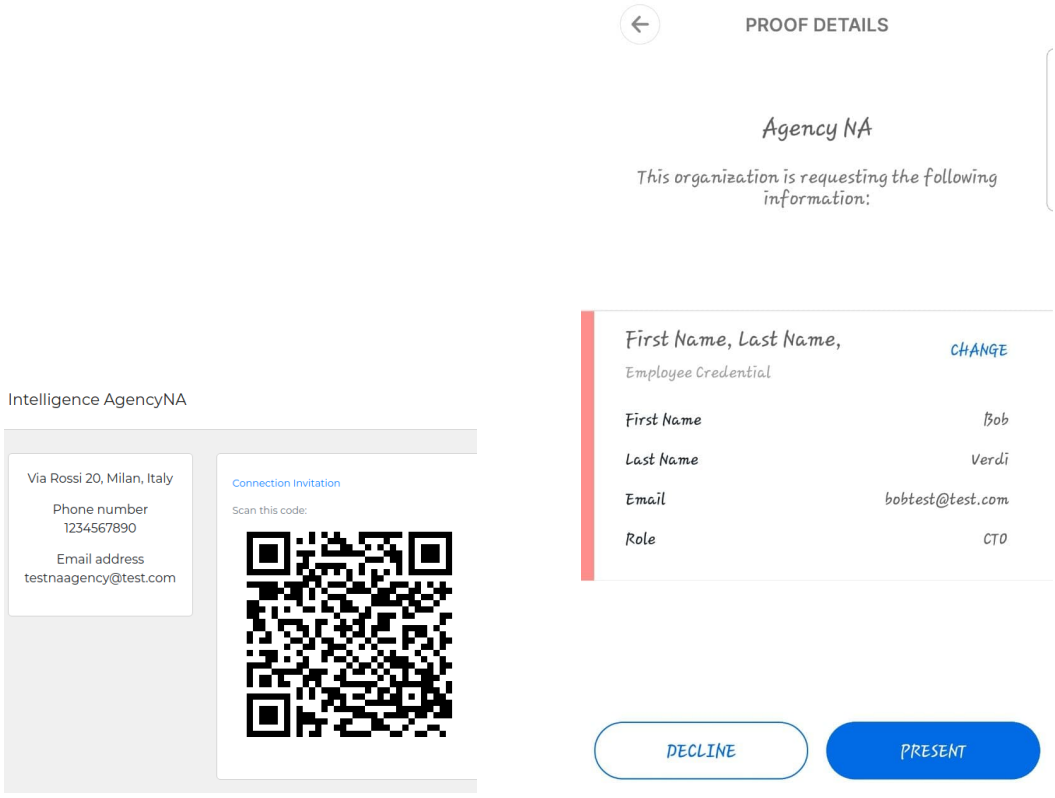
Figure 6. Overview of the Employee Credential (**a**) and X Credential Verification (**b**).

Once this Verification is created, Bob can set up a secure peer-to-peer connection with NA to provide the "Employee credential". This is done by scanning a QR code properly generated in the reserved area of Bob as shown in Figure 7a. However, not all the fields of the credential are provided by Bob but just a verifiable presentation of it. For example, in the case shown in Figure 7b, the Verifiable presentation includes four of five fields of the credential.

At this point, NA interacts with the blockchain to verify the validity of the credential received by Bob. This is performed in the background on the web application. The snippet of the Python code that implements this function is reported in Listing 1.

Listing 1. Python function to check the validity of a credential.

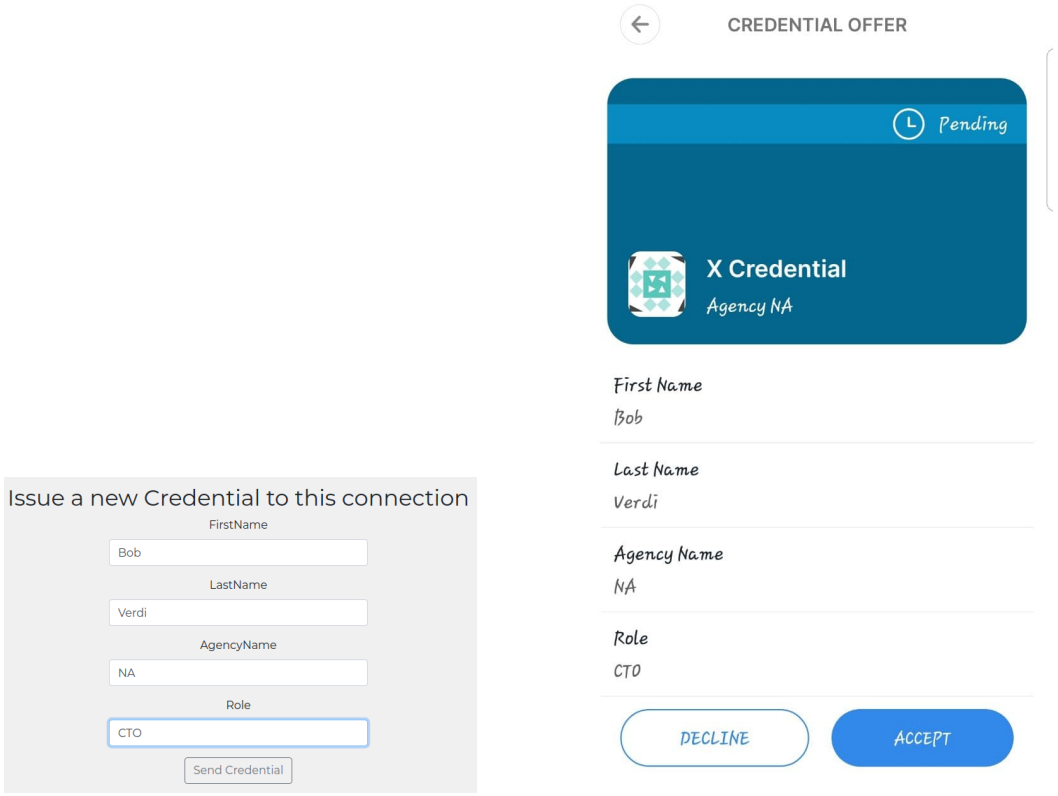
```
@app.route("/send_verification/<string:
connection_id>",
methods=["GET", "POST"])
def send_verification(connection_id):
connection_id = connection_id
policies =
credentials_client.
list_verification_policies()
policy_id = policies[0].policy_id
verification =
credentials_client.
send_verification_from_policy
(connection_id, policy_id)
return redirect(url_for
('verifications_connection',
connection_id=connection_id))
```



(**a**) QR Code. (**b**) Verifiable Presentation.

Figure 7. Overview of QR Code (**a**) and Verifiable Presentation (**b**).

Then, NA can release the "X credential" (see Figure 8a) that will appear on the mobile wallet of Bob (see Figure 8b).



(**a**) Issue of the X Credential. (**b**) X Credential on Bob's wallet.

Figure 8. Overview of the X Credential issuance process (**a**) and its storage in Bob's wallet (**b**).

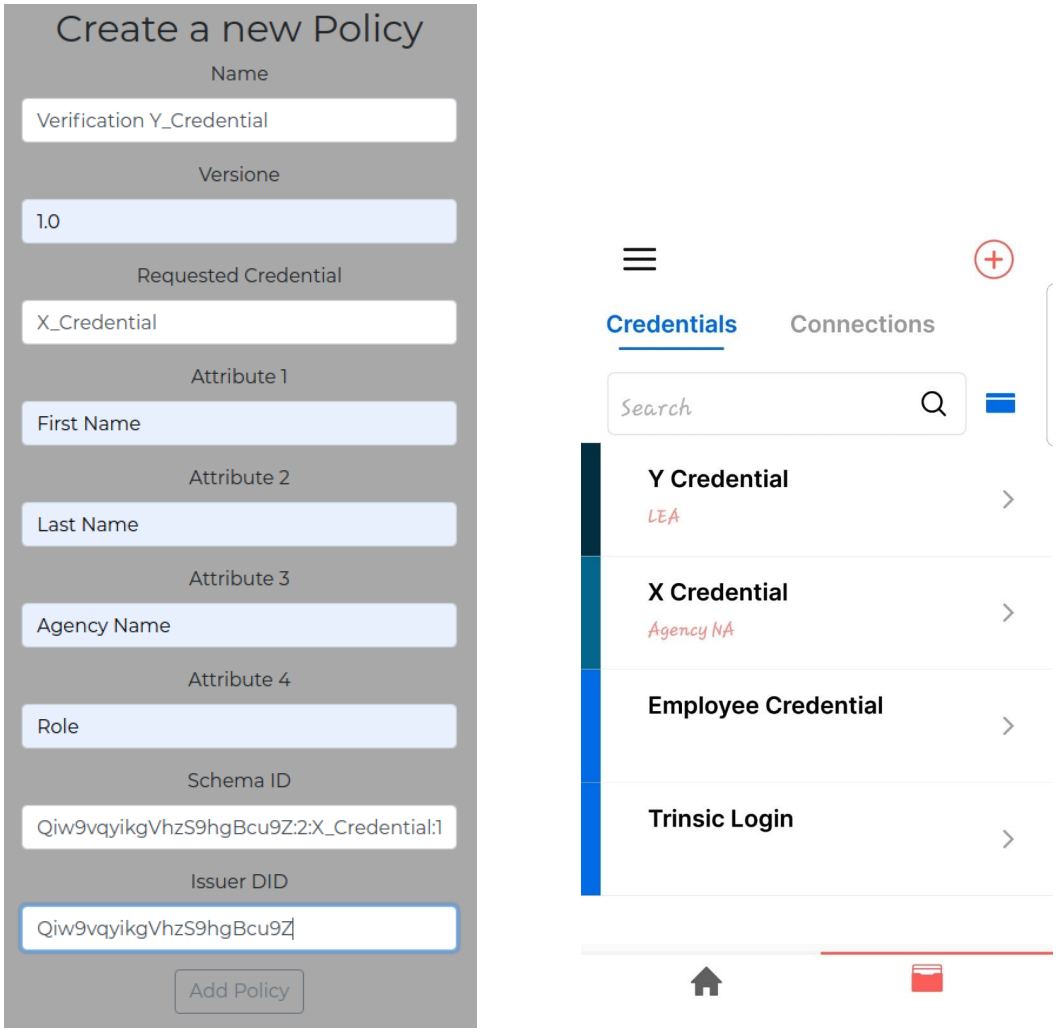
After obtaining the "X credential", Bob interacts with the LEA to get the "Y credential" for accessing the data on the LEMF. Similarly to the NA agency, the LEA generates a "Verification" for the "Y credential" through the dedicated web application (see Figure 9a). Observe that, among the fields required in this verification, there is the issuer DID of the entity releasing the "X credential" (i.e., the agency NA).

At this point, the procedure appears for Bob similar to the procedure performed with the NA agency. Indeed, Bob connects with the web application of the LEA and scans a QR code to provide the LEA with the Verifiable presentation of "X credential". However, a difference exists with the previous case. Indeed, such a presentation is not provided within a secure connection but is connectionless because the presentation of the "X credential" is required in order to establish the connection with the LEA. Once the "X credential" is verified by the LEA, it releases to Bob the "Y credential" (see Figure 9b) allowing him to interact with the LEMF. Specifically, Bob scans a QR code to establish a secure connection with the LEMF and provides it with a Verifiable presentation of the "Y credential". Then, Bob obtains the data of the LI procedure from the LEMF.

We conclude this section by discussing the data stored in the blockchain. Through the Indy Scan platform, it is possible to monitor all the transactions performed by an entity. Figure 10 shows a snapshot of the Indy Scan platform, which reports the transactions performed to build the necessary infrastructure for credential issuance and revocation. The fourth column of the table represents the issuer DID of the node originating the transaction, which is the agency NA. Specifically, we find the following transactions:

1. Tx 262048 and 262052 (SCHEMA): These transactions define the structure of two credentials: Employee Credential and X Credential, both set to version 1.0.
2. Tx 262049 and 262053 (CLAIM_DEF): Claim definitions associate the schemas (Employee Credential and X Credential) with the issuer's DID.

3. Tx 262054 (REVOC_REG_DEF): This transaction creates a revocation registry for a credential definition, specifying `ISSUANCE_BY_DEFAULT` as the issuance type and a registry capacity of 1024 entries.
4. Tx 262055 (REVOC_REG_ENTRY): This transaction logs an entry in the revocation registry, enabling tracking and management of the revocation status for issued credentials.



(**a**) Policy for the Y Credential. (**b**) Y Credential.

Figure 9. Overview of the policy for the Y Credential (**a**) and the Y Credential itself (**b**).

These transactions show the sequential process of decentralized credential management:

- Schemas define the data structure of credentials.
- Credential definitions connect schemas to issuers, facilitating the issuance of verifiable credentials.
- Revocation registries manage the status of issued credentials, promoting transparency and trust in the decentralized identity ecosystem.

Overall, this setup preserves the integrity of the credential lifecycle, allowing issuers, holders, and verifiers to interact securely within the Hyperledger Indy framework.

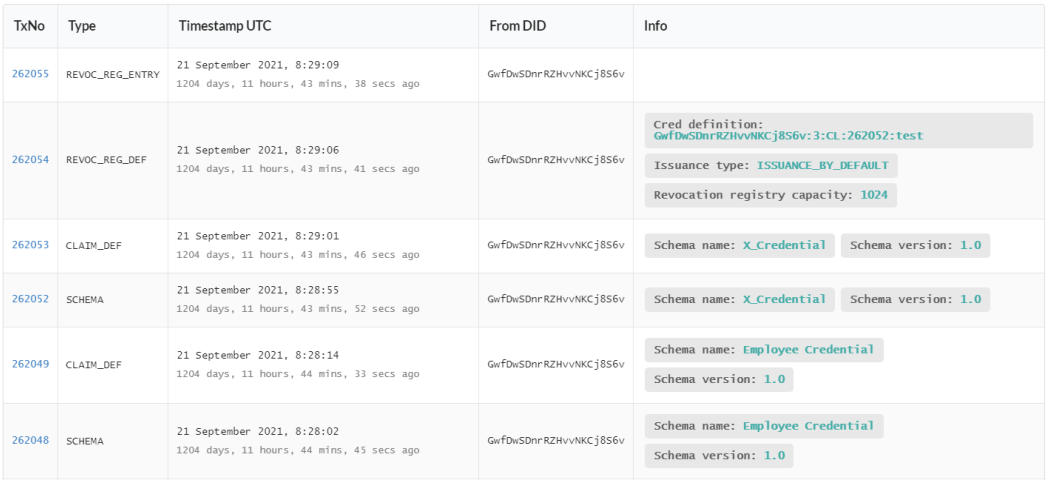


Figure 10. Indy Scan.

7. Related Work

Self-Sovereign Identity is an emerging paradigm attracting the interest of governments and enterprises [14,22,24,34,35]. One of the main benefits of the SSI paradigm is its compliance with the General Data Protection Regulation (GDPR) [36–39], making it an effective choice to develop privacy-by-design solutions. As a matter of fact, several concrete implementations of SSI frameworks are available to develop SSI-based solutions [31,40–42]. Among them, we rely on Sovrin [18,43–45], which is becoming a standard for deploying SSI solutions, as witnessed by several scientific papers [46–52] and industrial projects [53] proposing different solutions that utilize the Sovrin framework.

In the literature, several solutions have been proposed that apply the SSI approach to solve different problems in different domains. For example, some of these domains are healthcare [54–56], industrial IoT [57,58], and food supply chain [59].

In this paper, for the first time, we apply the SSI approach to the lawful interception domain. Lawful interception is an activity that involves legal [60–62], ethical [63], and technological issues [64,65]. From a technological point of view, several proposals, also recent [5,6,66], are available in the literature, especially in the field of telecommunication [67–70]. However, these works focus on the physical communication interfaces [70] and/or on the integrity and storage of the collected data [71].

This paper addresses a slightly different problem, which is access control in the LI procedure. To the best of our knowledge, previous solutions propose access control models (such as RBAC [19] or VACM [20]) at a theoretical level, but their implementations fail to enforce these models effectively, leaving access control unimplemented in practice.

8. Conclusions and Future Work

In this paper, we proposed an SSI-based solution to implement an access control mechanism that supports a LI procedure. Our proposal is motivated by the need to overcome the absence of a standard for the interactions between the LEA and LEMF. In the design of the solution, we followed the guidelines of the Sovrin framework. In particular, we adopted the SSI stack, which defines how trust is achieved among several participants. To make our proposal more concrete, we provided a proof of concept using standard and well-consolidated technologies, which allowed us to verify that our proposal is technically feasible.

The findings of this research show that an SSI-based solution can enhance security, automation, and interoperability in lawful interception procedures. Our proposal research defines how access control mechanisms in lawful interceptions can be strengthened, ensur-

ing that only authorized entities, specifically law enforcement agencies or external agencies, can retrieve intercepted data. This is particularly important in cross-border investigations, where secure access to intercepted communications is often hindered by differences in interception procedures across countries. Our solution eliminates the manual operations of traditional lawful interceptions, which are substituted by machine-readable procedures. This change reduces human error and improves efficiency by accelerating all the processes related to lawful interception. Moreover, the use of verifiable credentials mitigates the risks associated with centralized identity providers, reducing single points of failure and enhancing privacy through selective disclosure. By addressing the lack of standardized interaction protocols between LEA and LEMF, this research introduces a more secure and privacy-preserving approach to lawful interception and defines workflows for all involved entities, with the aim of improving investigative capabilities and enhancing legal compliance.

Alongside the advantages discussed above, our proposal presents some limitations. The first limitation concerns the adoption. Indeed, SSI is an emerging paradigm, which lacks widespread adoption and does not benefit from the sponsorship of major organizations (like Google and Facebook, which support federated identity). Moreover, the lack of uniform regulation regarding the use and validity of SSI makes legal compliance challenging, particularly in law enforcement, where adherence to legal frameworks is critical. Considering the eIDAS Regulation, although it is focused on government eIDs and does not integrate SSI, the success of blockchain convinced the EU Commission to revise regulations to consider the SSI paradigm [72]. Another limitation of our proposal concerns the introduction of operational costs. Since operations done on the blockchain require the payment of a transaction fee, this may change the business model. In our solution, each operation, such as credential issuance or verification, involves a blockchain transaction and incurs a small fee (usually around a few dollar cents), which is not necessary for traditional lawful interceptions. However, we expect that transaction fees introduced by our solution will be negligible compared to the overall costs incurred by organizations for lawful interception, as these expenses are primarily driven by infrastructure and human activity rather than identity and access control verification processes. Exploring these aspects is a natural progression of this research.

As further future work, we plan to integrate the SSI approach also in the interaction between the LEMF and the network operator. In particular, the technical parameters needed to start the LI procedure can be exchanged in the form of credentials through the peer-to-peer channels offered by the SSI approach. In other words, these channels may replace the HI1 management interface defined by the ETSI standard [10].

Author Contributions: Methodology, A.L.C., F.B., V.D.A. and A.L.; software, A.L.C. and A.L.; writing—original draft, A.L.C., F.B., V.D.A., A.L. and G.L.; writing—review and editing, A.L.C. and G.L.; supervision, F.B.; funding acquisition, G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by project SERICS (PE00000014—CUP H73C22000880001) under the MUR National Recovery and Resilience Plan funded by the European Union—NextGenerationEU. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The source code used in this research is available at https://github.com/CyberGoldSun/SSI_LI (accessed on 30 January 2025).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Doronin, V. "Lawful interception–A market access barrier in the European Union"? *Comput. Law Secur. Rev.* **2023**, *51*, 105867. [CrossRef]
2. Walters, R. Illegal Interception of Data. In *Cybersecurity and Data Laws of the Commonwealth: International Trade, Investment and Arbitration*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 267–274.
3. Omand, D. Examining the Ethics of Spying: A Practitioner's View. *Crim. Law Philos.* **2024**, *18*, 805–818. [CrossRef]
4. Li, G.; Ren, L.; Fu, Y.; Yang, Z.; Adetola, V.; Wen, J.; Zhu, Q.; Wu, T.; Candan, K.S.; O'Neill, Z. A critical review of cyber-physical security for building automation systems. *Annu. Rev. Control* **2023**, *55*, 237–254. [CrossRef]
5. Bultel, X.; Onete, C. Pairing-free secure-channel establishment in mobile networks with fine-grained lawful interception. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, Brno, Czech Republic, 25–29 April 2022; pp. 968–970.
6. Spiekermann, D.; Keller, J.; Eggendorfer, T. Improving Lawful Interception in Virtual Datacenters. In Proceedings of the Central European Cybersecurity Conference 2018, Ljubljana, Slovenia, 15–16 November 2018. [CrossRef]
7. Guhl, S.D.; Pendse, R. The Communications Assistance for Law Enforcement Act (CALEA). *Inf. Secur. Journal: Glob. Perspect.* **2008**, *17*, 110–113. [CrossRef]
8. 3GPP TS Working Group 33. Security architecture for Core Network and Terminals (Release 16). Technical Report 3GPP TS 33.108, 3rd Generation Partnership Project (3GPP). 2020. Available online: https://www.3gpp.org/ftp//Specs/archive/33_series/33.108/33108-f10.zip (accessed on 30 January 2025).
9. ITU-T Working Group Y.2770. Requirements for Deep Packet Inspection in Next Generation Networks. Technical Report ITU-T Y.2770, ITU-T (International Telecommunication Union—Telecommunication Standardization Sector), 2015. Available online: https://www.itu.int/rec/T-REC-Y.2770-201211-I (accessed on 30 January 2025).
10. ETSI (European Telecommunications Standards Institute.) Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic. Technical Report ETSI TS 101 671 V3.15.1, ETSI, 2018. Available online: https://www.etsi.org/deliver/etsi_ts/101600_101699/101671/03.15.01_60/ts_101671v031501p.pdf (accessed on 30 January 2025).
11. Turanjanin, V. When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach. *Int. Cybersecur. Law Rev.* **2023**, *4*, 115–136. [CrossRef]
12. Gorge, M. Lawful interception – key concepts, actors, trends and best practice considerations. *Comput. Fraud. Secur.* **2007**, *2007*, 10–14. [CrossRef]
13. Tobin, A.; Reed, D. The inevitable rise of self-sovereign identity. *Sovrin Found.* **2016**, *29*, 18.
14. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
15. Pöhn, D.; Grabatin, M.; Hommel, W. Analyzing the Threats to Blockchain-Based Self-Sovereign Identities by Conducting a Literature Survey. *Appl. Sci.* **2023**, *14*, 139. [CrossRef]
16. Buccafurri, F.; De Angelis, V.; Lazzaro, S.; Pugliese, A. Enforcing security policies on interacting authentication systems. *Comput. Secur.* **2024**, *140*, 103771. [CrossRef]
17. Naghmouchi, M.; Laurent, M.; Levallois-Barth, C.; Kaaniche, N. Comparative Analysis of Technical and Legal Frameworks of Various National Digial Identity Solutions. *arXiv* **2023**, arXiv:2310.01006.
18. Khovratovich, D.; Law, J. Sovrin: Digital identities in the blockchain era. *Github Commit Jasonalaw Oct.* **2017**, *17*, 38–99.
19. Ferraiolo, D.; Cugini, J.; Kuhn, D.R. Role-based access control (RBAC): Features and motivations. In Proceedings of the 11th Annual Computer Security Application Conference, New Orleans, LA, USA, 11–15 December 1995; pp. 241–248.
20. Wijnen, B.; Presuhn, R.; McCloghrie, K. RFC3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), 2002. Available online: https://datatracker.ietf.org/doc/html/rfc3415 (accessed on 30 January 2025).
21. Sovrin Governance Framework Working Group. Sovrin Glossary Appendix D. Available online: https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V2.pdf (accessed on 30 January 2025).
22. Satybaldy, A.; Ferdous, M.S.; Nowostawski, M. A taxonomy of challenges for self-sovereign identity systems. *IEEE Access* **2024**, *12*, 16151–16177. [CrossRef]
23. Davie, M.; Gisolfi, D.; Hardman, D.; Jordan, J.; O'Donnell, D.; Reed, D. The trust over ip stack. *IEEE Commun. Stand. Mag.* **2019**, *3*, 46–51. [CrossRef]
24. Preukschat, A.; Reed, D. *Self-Sovereign Identity*; Manning Publications: Shelter Island, NY, USA, 2021.
25. Buccafurri, F.; De Angelis, V.; Lazzaro, S. A Blockchain-Based Framework to Enhance Anonymous Services with Accountability Guarantees. *Future Internet* **2022**, *14*, 243. [CrossRef]
26. Ren, Y.; Liu, X.; Wu, Q.; Wang, L.; Zhang, W. Cryptographic accumulator and its application: A survey. *Secur. Commun. Netw.* **2022**, *2022*, 5429195. [CrossRef]

27. Helliar, C.V.; Crawford, L.; Rocca, L.; Teodori, C.; Veneziani, M. Permissionless and permissioned blockchain diffusion. *Int. J. Inf. Manag.* **2020**, *54*, 102136. [CrossRef]
28. Hardman, D. Aries RFC 0005: DID Communication. Available online: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0005-didcomm/README.md (accessed on 30 January 2025).
29. World Wide Web Consortium. Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web. 2019. Available online: https://www.w3.org/TR/vc-data-model/?#core-data-model (accessed on 30 January 2025).
30. Sovrin Governance Framework Working Group. Sovrin Governance Framework. Available online: https://sovrin.org/library/sovrin-governance-framework/ (accessed on 30 January 2025).
31. Bhattacharya, M.P.; Zavarsky, P.; Butakov, S. Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–7.
32. Trinsic. Welcome to Trinsic. Available online: https://github.com/trinsic-id (accessed on 30 January 2025).
33. Grinberg, M. *Flask Web Development: Developing Web Applications with Python*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2018.
34. Glöckler, J.; Sedlmeir, J.; Frank, M.; Fridgen, G. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Bus. Inf. Syst. Eng.* **2024**, *66*, 421–440. [CrossRef]
35. Soltani, R.; Nguyen, U.T.; An, A. A Survey of Self-Sovereign Identity Ecosystem. *Secur. Commun. Netw.* **2021**, *2021*, 8873429. [CrossRef]
36. Shehu, A.S. On the Compliance of Self-Sovereign Identity with GDPR Principles: A Critical Review. *arXiv* **2024**, arXiv:2409.03624.
37. Voigt, P.; Von dem Bussche, A. The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10, pp. 10–5555.
38. Naik, N.; Jenkins, P. Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity. In Proceedings of the 2020 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, UK, 5–7 November 2020; pp. 1–6.
39. Kondova, G.; Erbguth, J. Self-sovereign identity on public blockchains and the GDPR. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, 30 March 30–3 April 2020; pp. 342–345.
40. Naik, N.; Jenkins, P. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020; pp. 1–7.
41. Stokkink, Q.; Ishmaev, G.; Epema, D.; Pouwelse, J. A truly self-sovereign identity system. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 1–8.
42. Grüner, A.; Mühle, A.; Meinel, C. An integration architecture to enable service providers for self-sovereign identity. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28 September 2019; pp. 1–5.
43. Pava-Díaz, R.A.; Gil-Ruiz, J.; López-Sarmiento, D.A. Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation. *Front. Blockchain* **2024**, *7*, 1443362. [CrossRef]
44. Windley, P.J. Sovrin: An identity metasystem for self-sovereign identity. *Front. Blockchain* **2021**, *4*, 626726. [CrossRef]
45. Reed, D.; Law, J.; Hardman, D. The Technical Foundations of Sovrin. 2016. Available online: https://sovrin.org/wp-content/uploads/2017/04/The-Technical-Foundations-of-Sovrin.pdf (accessed on 30 January 2025).
46. López, D.; Farooq, B. A multi-layered blockchain framework for smart mobility data-markets. *Transp. Res. Part C Emerg. Technol.* **2020**, *111*, 588–615. [CrossRef]
47. Bartolomeu, P.C.; Vieira, E.; Ferreira, J. Pay as You Go: A Generic Crypto Tolling Architecture. *IEEE Access* **2020**, *8*, 196212–196222. [CrossRef]
48. Barros, M.d.V.; Schardong, F.; Custódio, R.F. Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass. *arXiv* **2022**, arXiv:2202.09207.
49. Ahmed, F.; Hussain, S.A. A Privacy-Preserving Cross-domain Network access Services Using Sovrin Identifier. In Proceedings of the 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 23–25 November 2021; pp. 30–37. [CrossRef]
50. Helminger, L.; Kales, D.; Ramacher, S.; Walch, R. Multi-party revocation in sovrin: Performance through distributed trust. In Proceedings of the Cryptographers' Track at the RSA Conference, Virtual Event, 17–20 May 2021; pp. 527–551.
51. Abraham, A.; Theuermann, K.; Kirchengast, E. Qualified eID Derivation Into a Distributed Ledger Based IdM System. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1406–1412. [CrossRef]
52. Grabatin, M.; Hommel, W. Self-sovereign Identity Management in Wireless Ad Hoc Mesh Networks. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Virtual Conference, 17–21 May 2021; pp. 480–486.

53. Sovrin Foundation. Use Case Archives. Available online: https://sovrin.org/category/use-cases/ (accessed on 30 January 2025).
54. Ling, A.; Butakov, S. Trust Framework for Self-Sovereign ID in Metaverse Health Care Applications. *Data Sci. Manag.* **2024**, *7*, 304–313. [CrossRef]
55. Shuaib, M.; Alam, S.; Alam, M.S.; Nasir, M.S. Self-sovereign identity for healthcare using blockchain. *Mater. Today Proc.* **2023**, *81*, 203–207. [CrossRef]
56. Bai, P.; Kumar, S.; Aggarwal, G.; Mahmud, M.; Kaiwartya, O.; Lloret, J. Self-sovereignty identity management model for smart healthcare system. *Sensors* **2022**, *22*, 4714. [CrossRef] [PubMed]
57. De Diego, S.; Regueiro, C.; Macia-Fernandez, G. Enabling identity for the IoT-as-a-service business model. *IEEE Access* **2021**, *9*, 159965–159975. [CrossRef]
58. Bartolomeu, P.C.; Vieira, E.; Hosseini, S.M.; Ferreira, J. Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 10–13 September 2019; pp. 1173–1180.
59. Cocco, L.; Tonelli, R.; Marchesi, M. Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain. *Future Internet* **2021**, *13*, 301. [CrossRef]
60. Bronitt, S.; Stellios, J. Telecommunications interception in Australia: Recent trends and regulatory prospects. *Telecommun. Policy* **2005**, *29*, 875–888. [CrossRef]
61. Abelson, H.; Anderson, R.; Bellovin, S.M.; Benaloh, J.; Blaze, M.; Diffie, W.; Gilmore, J.; Green, M.; Landau, S.; Neumann, P.G.; et al. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *J. Cybersecur.* **2015**, *1*, 69–79. [CrossRef]
62. Brown, I. Lawful interception capability requirements. *Comput. Law,* **2013**. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309413 (accessed on 30 January 2025).
63. Christen, M.; Gordijn, B.; Loi, M. *The Ethics of Cybersecurity*; Springer Nature: Berlin/Heidelberg, Germany, 2020. Available online: https://library.oapen.org/handle/20.500.12657/47324 (accessed on 30 January 2025).
64. Cajani, F. "All along the watchtower": Matters not yet solved regarding communication interception systems and electronic data retained on foreign servers. In *Handling and Exchanging Electronic Evidence Across Europe*; Springer: Cham, Switzerland, 2018; pp. 59–71.
65. Pleva, M.; Cizmar, A.; Dobos, L. Voice Quality Measuring Setup with Automatic Voice over IP Call Generator and Lawful Interception Packet Analyzer. *J. Electr. Electron. Eng.* **2012**, *5*, 191.
66. Buccafurri, F.; Consoli, A.; Labrini, C.; Nesurini, A.M. A Solution to Support Integrity in the Lawful Interception Ecosystem. In *International Conference on Electronic Government and the Information Systems Perspective*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 21–33.
67. Xu, X.; Jia, W.K.; Wu, Y.; Wang, X. On the Optimal Lawful Intercept Access Points Placement Problem in Hybrid Software-Defined Networks. *Sensors* **2021**, *21*, 428. [CrossRef] [PubMed]
68. Branch, P.; Pavlicic, A.; Armitage, G. Using MAC addresses in the lawful interception of IP traffic. In Proceedings of the Australian Telecommunications Networks & Applications Conference (ATNAC), Sydney, Australia, 8–10 December 2004; pp. 9–11.
69. Karpagavinayagam, B.; State, R.; Festor, O. Monitoring architecture for lawful interception in VoIP networks. In Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP 2007), San Jose, CA, USA, 1–5 July 2007; p. 5.
70. Aljaž, T.; Imperl, B.; Švigelj, A. Border gateway function performance requirements for the lawful intercept of voice at IMS architecture. *AEU-Int. J. Electron. Commun.* **2008**, *62*, 610–621. [CrossRef]
71. Muñoz, A.; Urueña, M.; Aparicio, R.; Rodríguez de los Santos, G. Digital Wiretap Warrant: Improving the security of ETSI Lawful Interception. *Digit. Investig.* **2015**, *14*, 1–16. [CrossRef]
72. Alamillo, D.I.; Schwalm, S. Self-Sovereign-Identity & eIDAS: A Contradiction? Challenges and Chances of [eIDAS2]. *Eur. Rev. Digit. Adm. Law* **2021**, *2*, 89–108.