Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

Article

Decentralized Identity With Applications to Security and Privacy for the Internet of Things

Chalima Dimitra Nassar Kyriakidou[1,*], Athanasia Maria Papathanasiou[1,*] and George C. Polyzos[1,2,*]

[1]Mobile Multimedia Laboratory, Department of Informatics, School of Information Sciences and Technology, Athen University of Economics and Business, 10434 Athens, Greece
[2]Internet Identity, Security and Privacy Solutions P.C. (ExcID), 11362 Athens, Greece
E-mail: dnassar@aueb.gr; sissypapathanasiou@aueb.gr; polyzos@aueb.gr

Received: 16 May 2023; **Revised:** 5 July 2023; **Accepted:** 14 July 2023

Abstract: Decentralized Identity (dID) has brought to the forefront the advantages and importance of total user control over identity. Previous solutions delegate identity management to the responsibility of third-party applications or services, which may raise multiple privacy and security concerns regarding users' personal data. In this paper, we highlight the significance of dID and in particular Self-Sovereign Identity (SSI) for a rapidly evolving ecosystem with a plethora of interconnected devices with different characteristics, such as the Internet of Things (IoT). Specifically, we analyze the benefits of incorporating SSI principles and technologies in IoT environments, while also discussing the challenges that may be introduced when combining the complexity of SSI concepts with the diverse and large-scale IoT environment. In addition, we present a thorough overview of existing systems that integrate SSI components into IoT environments, in order to address the challenges of authentication, authorization, and access control even for constrained IoT devices. Finally, we provide a comprehensive analysis regarding the contributions of Decentralized Identifiers and Verifiable Credentials, the two main pillars of SSI, for enhanced privacy and security for the Internet at large and for the IoT in particular.

Keywords: Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), authentication, authorization, access control, personal data

1. Introduction

The widespread deployment of the Internet of Things (IoT) has brought about the possibility of transforming our interaction with the physical world by interconnecting everyday devices to the Internet and facilitating their data exchange not only with each other but also with humans. In particular, the number of IoT devices is expected to increase from 20.4 billion in 2020 to 75.0 in 2025 (https://review42.com/resources/internet-of-things-stats/). With the rising prevalence of IoT deployments, there is an expanding urgency to establish strong privacy and security measures. The number of interconnected devices in these deployments, their placement in the environment, often widely accessible, their typically unattended operation, and the sheer volume of data produced makes them susceptible to malicious attacks and unauthorized access [1], emphasizing the need for robust protection. Specifically, 112.24 million IoT attacks were encountered in 2022 (https://www.zippia.com/advice/internet-of-things-statistics/). Decentralized identity (dID) systems, which encompass a broader set of principles for managing digital identities in a decentralized manner, offer a promising approach to addressing these concerns. By empowering individuals with greater control over their personal data and identity information, dID systems reduce reliance on centralized identity providers.

DOI: https://doi.org/10.37256/cnc.1220233048

In this paper, we delve into the concept of dID and its potential for enhancing security and privacy in the IoT ecosystem. Integrating dID systems into the IoT ecosystem seems to be a promising solution, as by 2030, at least 80% of EU citizens are expected to have a digital identification system (https://www.electronicid.eu/en/blog/post/eidas-2-0-what-can-companies-expect-from-it/en). We begin with a brief overview of the evolution of identity, starting from human identity and tracing its trajectory to the development of centralized identity systems, followed by subsequent advancements in federated identity systems. We will also emphasize the significant contribution of the Web of Trust (WoT) in the evolution of identity. Subsequently, we will discuss how the evolution of identity has progressed towards a user-centric model, where authentication and authorization protocols like OAuth, FIDO, and OpenID, further contributed to the development of the Self-Sovereign Identity (SSI) concept. Finally, we provide a definition for SSI, the latest development in the history of digital identity, as a decentralized approach to identity management that puts users in control of their personal data, allowing them to manage their identities independently of centralized authorities and intermediaries. Furthermore, we present an overview of the typical SSI ecosystem, analyze its architecture from a Peer-to-Peer (P2P) perspective, and examine the role of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs).

In all identity systems, it is essential to have a reliable way of representing entries with unique identifiers. This requirement remains applicable to dID systems, where DIDs assume a fundamental role in representing individuals, entities or items within the system. A DID is a unique identifier that allows individuals or entities to create and control their own identity on a decentralized network, which is a fundamental component of the SSI framework. The significance of DIDs lies in their role of uniquely representing entries within the dID ecosystem. This parallels the importance of usernames or email addresses in centralized systems, where they serve as primary means to identify and distinguish users. In this paper, we provide a comprehensive explanation of DIDs and their significance in a dID system, including their format and how they can be resolved to retrieve the corresponding DID documents (which provide relevant metadata). Additionally, we examine different DID methods and the role of DID Auth in enabling users to authenticate their identity to IoT devices and services.

Moreover, we present the concept of VCs, digital credentials that represent the same information with their respective physical documents and consist of a set of verifiable claims regarding a subject, such as name, age, address and current employment. In the following sections we analyze the structure of VCs, we refer to Verifiable Presentations (VPs), which can be defined as two or more VCs that will be presented to a third party for verification purposes, and finally we examine the concepts of selective disclosure and credential revocation. In particular, we divide revocation into three categories, namely, centralized, decentralized, and Zero Knowledge Proof (ZKP) based revocation, while also outlining the importance of selective disclosure for VCs, as subjects can easily choose which data to disclose to a third party, without revealing any additional information.

The European Blockchain Services Infrastructure (EBSI) has become a significant contributor to the development of dID solutions. It aims to create a trusted and secure ecosystem for cross-border digital public services, and identity is a key component of this vision. For this reason, it has established its own dID framework using DIDs and VCs, which conform to World Wide Web Consortium (W3C) standards. Additionally, EBSI has also implemented a variety of use cases, in order to demonstrate the practical application and efficiency of its framework. In this paper, we analyze a Track and Trace Use Case, which utilizes DIDs and VCs to track the authenticity and origin of documents and potentially goods in a supply chain.

Another notable initiative is the Digital Product Passport, which aims to provide a standardized way to share product information across borders and value chains, through VCs. EBSI is also collaborating with the European Commission to develop European Digital Identity (EUDI) Wallets, which would allow citizens to store and manage their identity information in a secure and privacy-preserving manner. Finally, EBSI's decentralized trust model, based on a network of trusted nodes, fits well with the Web 3.0 trust model and could provide a secure foundation for emerging IoT ecosystems.

As previously mentioned, the IoT refers to a vast network of interconnected devices, objects, and systems that can collect, exchange, analyze and even act upon data in real-time. We present a simplified architecture of an IoT ecosystem and we examine how IoT systems would be impacted by the incorporation of d dID management solutions, which are better suited for the highly distributed and heterogeneous nature of IoT networks. This paper also explores the benefits, challenges, and contributions to the privacy and security of utilizing SSI for IoT environments, some of which are derived from previous research in this area [2–10].

The remainder of this paper is organized as follows. In Section 2 we provide a survey of dID Technologies and emphasize their key properties. In Section 3 we present applications of dID and in particular SSI technologies to the IoT, based on various published proposals and discuss their impact on security and privacy. In Section 4 we analyze the benefits of introducing SSI solutions to IoT applications and uncover new

challenges that are introduced. In Section 5 we focus on SSI contributions to security and privacy in the IoT. Finally, in Section 6, we conclude with a summary and brief outlook.

2. Decentralized Identity Technologies

SSI is a type of dID system that gives individuals control over their personal information and how it is shared, stored, and accessed. SSI has emerged as a revolutionary concept that has the potential to reshape the way we manage and control our digital identities. SSI is based on the idea that individuals should have complete ownership and control over their digital identities, rather than relying on centralized authorities to manage their personal data. It can empower individuals to engage in secure and privacy-preserving interactions, facilitating trusted collaborations, transactions, and exchanges of information. DIDs and VCs are key components of SSI that enable secure and trustworthy interactions between entities.

SSI is necessary due to the increasing concerns around privacy, security, and data ownership in the digital world. Traditional identity management systems often rely on centralized authorities, such as government agencies or corporations, to control and verify individuals' identities. This centralized approach poses risks, as these authorities become single points of failure and potential targets for data breaches. Additionally, individuals have limited control over how their personal information is used and shared, leading to privacy concerns and potential misuse of data by unauthorized parties. SSI and dID systems in general, prioritize data privacy, which leads to the minimization of the risk of falling victim to identity theft, fraud, or other forms of cyberattacks. They allow users to decide what information is shared, with whom, and for what purposes. This means that it allows users to avoid unnecessary data collection, profiling, or targeted advertising by centralized authorities, ensuring that users' personal information is used in ways that align with their preferences and values.

A prime example of how dID and SSI systems can be critically beneficial for and applied to social networking, in order to offer users full control over their digital identities, autonomy and improved privacy, is the recent move away of many users from Twitter (https://www.theguardian.com/technology/2022/nov/08/how-to-quit-twitter-and-where-to-go-instead, https://digiday.com/marketing/considering-leaving-twitter-heres-a-roundup-of-alternatives) mostly towards Mastodon (https://joinmastodon.org) and the inception, design, and development of Bluesky Social (https://bsky.app and https://blueskyweb.xyz/blog, informally referred to as decentralized Twitter), backed by the ex-CEO of Twitter, Jack Dorsey.

Unlike traditional social media platforms, like Twitter, Mastodon is decentralized, utilizing multiple interconnected servers, known as instances, to form a network. Each instance has its own community and set of rules, allowing users to choose an instance that aligns with their preferences. Users are able to create an account on any instance within the network and their identity is not tied to a single centralized authority. This means that they can interact with users from other instances, fostering a distributed and interconnected social experience. Additionally, in Mastodon users have the ability to import and export their data, migrate between instances or even host their own instance with their own rules and policies. This way users have autonomy over their identities and their data remains within their control. In contrast, users with accounts on centralized platforms are reliant on the platform provider for identity and data management and portability.

As users were leaving Twitter at the end of 2022 and early 2023, many for Mastodon, one problem that surfaced was that they had no easy way to connect with their followers and other users also leaving Twitter for other social networks and in particular Mastodon. Their digital identity and their connections were tied to Twitter. Furthermore, the problem of controlling someone's identity persists even in Mastodon, where the identity is defined with respect to individual servers; if the server fails, or is decommissioned ungracefully, then the identity problem appears and is no different than that of centralized systems. If the server goes away gracefully, there are processes defined to hand over the identity, relying on another server.

On the other hand, Bluesky Social chose to exploit DIDs in order to enable SSI and identity portability (https://github.com/bluesky-social/did-method-plc). Bluesky Social is still in Beta and limits the number of users, therefore the impact of this design choice is not yet clearly apparent, but it seems to be a modern and correct choice.

2.1 *The Evolution of Digital Identity*

In this section, we will delve into the evolution of SSI, by beginning with the concept of identity and progressing to digital identity. While we will only provide a brief overview of a few key developments in the history of identity, it should be noted that Christopher Allen [11] has conducted a more thorough analysis of this topic. We will outline the crucial forms of identity that have emerged over time and highlight the significance of SSI as the latest development in this progression. In addition, we will introduce the principles to which SSI

systems must conform, as well as present the SSI architecture. The historical background of SSI is depicted in Figure 1.

Human Identity From the beginning of human history, the need for humans to distinguish themselves from others has been evident. The human identity, as it is now understood, comprises characteristics such as first name, last name, place and date of birth, and is provided by the government to each citizen in the form of IDs, passports, and other such documents.

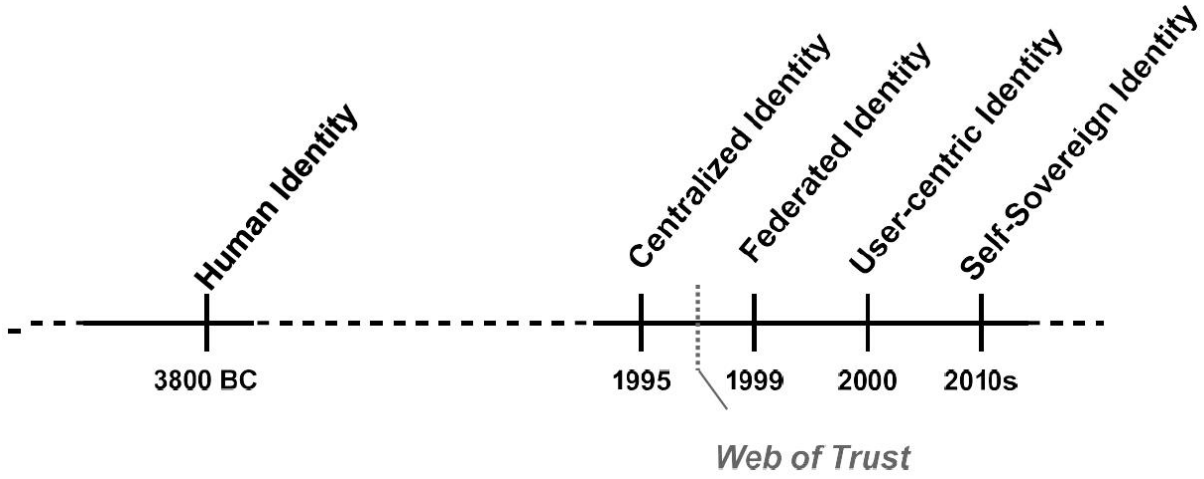

Figure 1. The evolution of Digital Identity

Centralized Identity In real-world scenarios, the identification of individuals was traditionally facilitated by centralized entities, usually governmental bodies, which were responsible for the creation, modification, verification, and revocation of such identities. The continuity of the pattern of centralized identity management persisted with the advent of the Internet, compelling users to manage multiple identities to access different websites or online services. Organizations such as Internet Assigned Numbers Authority (IANA) [12], Internet Corporation for Assigned Names and Numbers (ICANN) [13], and certificate authorities (CAs) [14] were established to validate IP addresses, mediate domain names, and assist e-commerce sites in verifying their identity.

Federated Identity The initial breakthrough in digital identity was Federated Identity. It is a system of mutual trust established among multiple organizations or online entities, allowing users to use a single digital identity across various websites or services. The failure of federated identity can be pinpointed to the fact that even though users have gained some level of control over their digital identity, this control is still subject to the authority of the federated entity and could potentially be revoked at any time. It is significant to mention that just before the era of Federated Identity, in 1999, Pretty Good Privacy (PGP) made a noteworthy contribution to SSI by introducing the WoT, which, according to Caronni [15], enabled peers to validate and introduce public keys, thus establishing trust for a digital identity. However, its focus on email addresses meant that it still relied on centralized hierarchies and had limited adoption.

User-Centric Identity The concept of User-Centric Identity marked a significant step toward recognizing the necessity of SSI. User-centric methodologies prioritized user consent and interoperability. Projects linked to this form of digital identity envisioned that, eventually, each person would be able to manage their digital identity. According to Motykowski et al. [16], during the Internet Identity Workshop in 2005, the concept of User-Centric Identity was introduced with the objective of developing an identification method that would be continuous and not subject to reassignment to a different user, unlike email addresses or phone numbers. It is worth noting that the concept of User-Centric Identity was initially proposed by the Augmented Social Network (ASN), circa 2000. This is documented in the white paper by Jordon et al. [17]. Although the exact term is not mentioned, they proposed incorporating a persistent, online identity as an integral part of the Internet's architecture. New approaches to digital identity emerged as a result, including OAuth, FIDO and OpenID, which are documented by Kahrs et al. [18]. A comparison of the aforementioned approaches is provided in Table 1.

Table 1. Comparison Table for OAuth, FIDO and OpenID.

Protocol	Purpose	Key Features	VC Integration
OAuth	User grants access without sharing credentials	Utilizes access tokens	√
FIDO	Secure, private, user-friendly protocols	Offers password-less authentication (UAF) and FIDO Security Keys (U2F)	√
OpenID	User chooses IDP to sign-in to different websites	Supports JWTs as access tokens	√

OAuth protocol OAuth is a security protocol that enables users to grant access to their digital identity to a third-party application or service without compromising their security credentials [19]. The conventional client-server authentication model is a method used to grant access to protected resources on a server, by requiring users that make requests for it, to authenticate with the server through their credentials. Although this traditional approach aims to ensure that only authorized users will be granted access to restricted resources, it raises several security concerns regarding the end user's digital identity. OAuth addresses these issues by ensuring that users are not required to share their credentials with third party applications. In accordance with the specification [20], OAuth 1.0, an earlier version of the OAuth protocol, operates by requiring the user to sign an authorization request with a shared secret, in order to grant permission to a third-party application to access protected resources on a resource server. Whereas in OAuth 2.0, this is achieved through the utilization of access tokens, which are strings that specify certain attributes, such as the scope and lifetime, for accessing the resources. Specifically, an authorization server issues access tokens to third-party clients upon obtaining consent from the resource owner. Access tokens are subsequently used by clients to gain access to the protected resources hosted on the resource server. OAuth 2.0 has mostly superseded its predecessor, as a result of its more adaptable and simpler architecture. Fotiou et al. [21] present a notable usage of the OAuth 2.0 protocol in an authentication system that is relevant to the context of this article, as it involves the incorporation of VCs. Briefly, the aforementioned system achieves continuous authorization of HTTP requests by leveraging VCs and OAuth 2.0.

Fast Identity Online FIDO [22] is an open standard that seeks to enhance the security and user experience of online authentication. It aims to provide an alternative to conventional password-based authentication mechanisms by implementing authentication protocols that are secure, private, and user-friendly. The FIDO Alliance has specified two protocols that utilize public-key cryptography and leverage biometric authentication methods. FIDO Universal Authentication Framework (FIDO UAF) supports password-less authentication from smart devices. Specifically, it involves the use of a device carrying a FIDO UAF stack, which enables users to register their devices to an online service by selecting a biometric or local authentication mechanism, such as fingerprint, face or voice recognition, entering a PIN and even a combination of various authentication methods. The FIDO Universal Second Factor (FIDO U2F) protocol provides an additional layer of security to the existing password-based authentication system. It enables online services to enhance the security of their authentication process by requiring a strong second factor, such as a FIDO Security Key. This strong second factor allows the service to adopt simpler password policies, such as PINs, without compromising security. Both FIDO UAF and FIDO U2F protocols have been integrated and standardized by the W3C as the Web Authentication Recommendation (FIDO2). Chadwick et al. [23] propose a notable implementation for UK NHS patients that leverages both FIDO and VCs for tasks such as appointment management and prescription orders. The conducted research demonstrates the user-friendly nature of the proposed system and the superiority of local or biometric authentication methods over the use of conventional credentials. This, by extension, underscores the potential of FIDO to address the challenges posed by Federated Identity Management systems.

OpenID protocol OpenID [24] is an authentication protocol that enables users to create an account with an identity provider (IDP) and use it to sign in to multiple websites or applications that support OpenID authentication, thus eliminating the need for users to manage different credentials for different websites. Users choose their preferred provider for authentication and if they select a website that is reliable, they can experience many of the benefits of SSI. It can be argued that OpenID is the digital identity system that is most similar to SSI [25]. However, the registration of an OpenID necessitates technical skills and expertise, and the registering entity holds the authority to withdraw it at any given moment. Additionally, it is of significance to note that it allows any organization or individual to become an OpenID provider. OpenID 2.0 [26] is a revised and enhanced version of the initial OpenID protocol that offers improved security and functionality in comparison to its predecessor. Briefly, the newer version of OpenID introduced several improvements, one of which was an enhanced approach for discovering the user's IDP through Yadis, as opposed to the previous method that relied on URL patterns to identify the provider. Additionally, in terms of extensibility, OpenID 2.0 offered an enhanced framework that enabled the addition of new features to the protocol with greater ease, thus enabling the incorporation of new mechanisms for authentication and authorization in a more streamlined

manner. OpenID Connect [27] is an updated version of OpenID that expands its functionality for authentication and authorization by incorporating features like support for OAuth 2.0 and JSON Web Tokens (JWTs). Its primary purpose is to offer a standard protocol for applications to obtain user data from IDPs. OpenID Connect, being based on the OAuth 2.0 framework, allows for the use of VCs [28], which are utilized as a type of access token, specifically for authentication of a user's identity or for granting access to specific resources or services. OpenID Connect achieves this by supporting the exchange of access tokens, which can be in the form of JWTs, thereby enabling secure and privacy-preserving authentication and authorization functionalities.

2.2 *Self-Sovereign Identity*

The introduction of User-Centric designs enabled the transformation of centralized identities into interoperable federated identities while ensuring some degree of user consent over identity sharing. However, the SSI system required going beyond user consent and allowing users to have full control over their identities, including their creation, management, and sharing.

Devon Loffreto [29] was among the earliest individuals to discuss the concept of sovereignty, around 2012. He emphasized that true sovereignty cannot exist when there is a requirement for national registration. SSI was further proliferated by several "personal Cloud" initiatives that emerged around the same time. Over the years, SSI has been approached from various perspectives, including a mathematical perspective by Devon Loffreto [30], a legal perspective by Respect Network [31] and Smith et al. [32], and an international perspective by Dahan et al. [33]. The architecture of SSI is depicted in Figure 2.

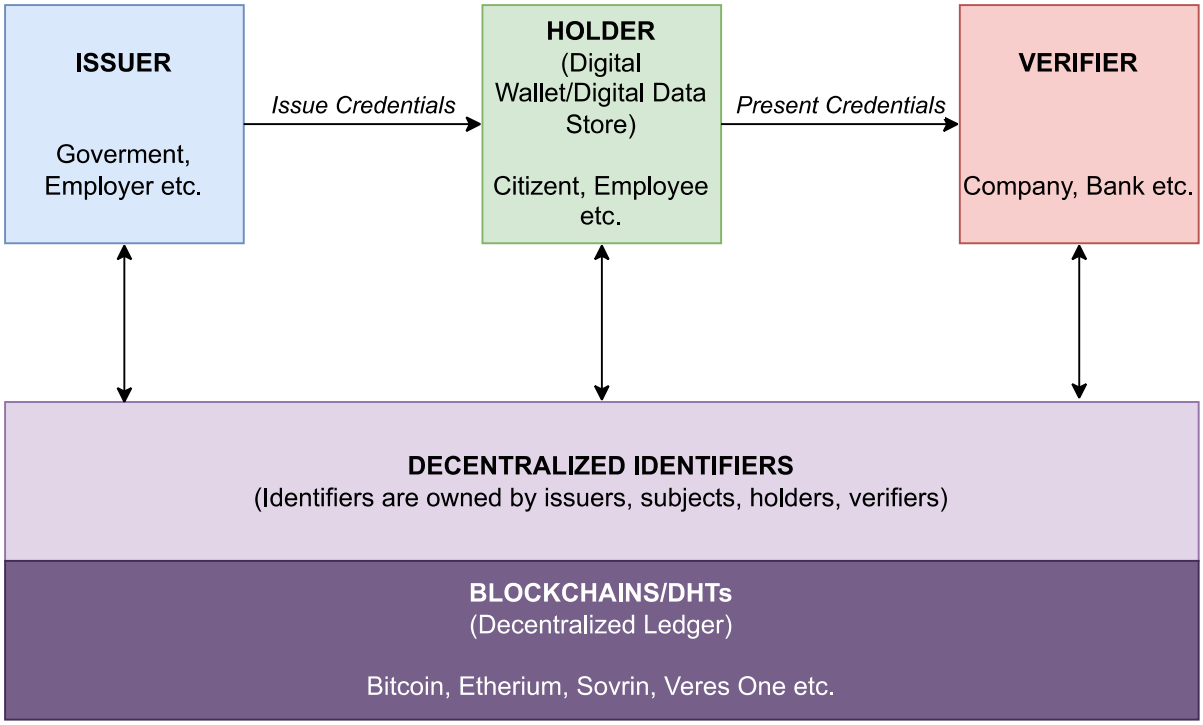

Figure 2. SSI Architecture.

In order to strike a balance between safeguarding individual interests and supporting the common good, while maintaining transparency and fairness, Christopher Allen proposed 10 principles that must be followed by any SSI system [11]. Namely, Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimalization and Protection. Christopher Allen has urged individuals in the digital identity community to incorporate and revise these principles, with some updates and **critiques** having already been proposed [34]. The Sovrin Foundation has made a noteworthy contribution by categorizing these principles into three groups: security, controllability, and portability [35]. The security group includes principles that emphasize the need to keep identity information secure. The controllability group encompasses principles that emphasize the importance of giving users control over who can access their data. Finally, the portability group includes principles that emphasize the importance of enabling users to use their identity data freely, without being tied to a single provider.

SSI is a distinct model characterized by a P2P architecture, which is illustrated in Figure 3 and facilitated by blockchain technology, which provides attributes such as global uniqueness, high availability, cryptographic verifiability, and the absence of central authority. Thus, within the SSI architecture, the identity of an individual, group, or connected device is defined by the relationships established with other peers, which could be individuals, groups, or other connected devices. These relationships are established through connections, while the digital wallet situated at the end of these connections stores keys, credentials, and tokens. The credentials stored in the wallet are issued by different peers, including entities such as passport offices, driver's license authorities, employers, and loyalty programs. When a user needs their identity or credentials to be verified, they initiate a connection with another peer and share one or more credentials, which undergo verification using public keys and DIDs, often recorded on a ledger.

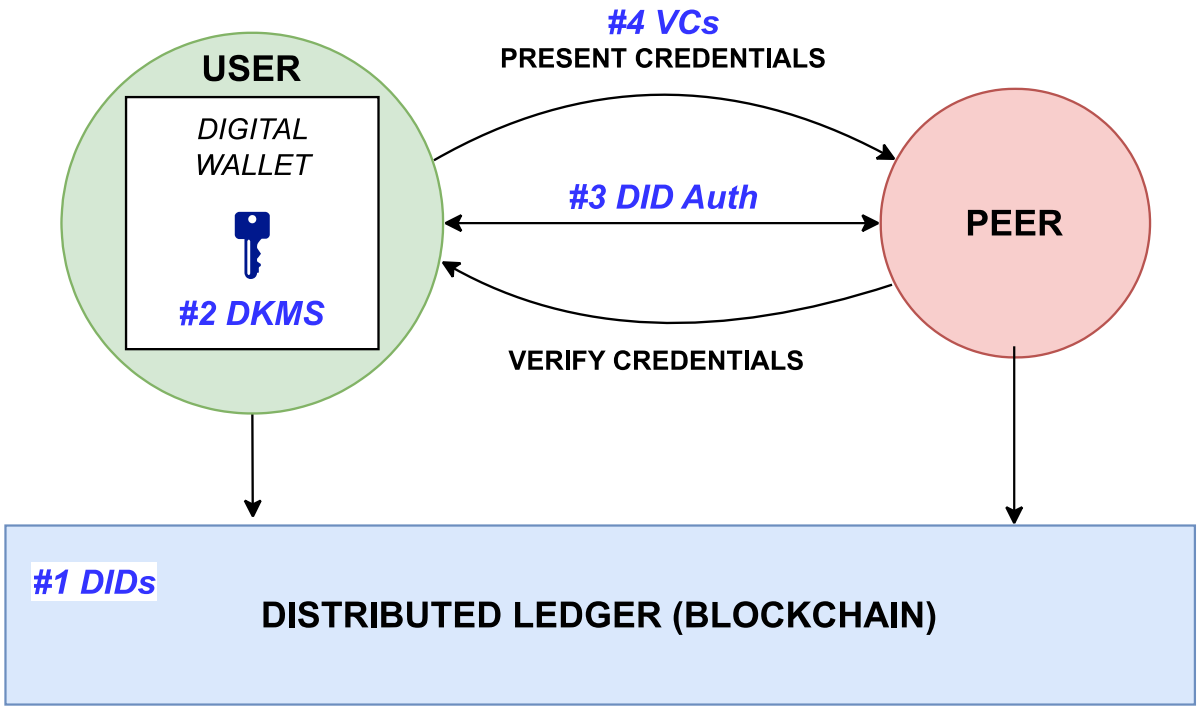

Figure 3. SSI Peer-to-Peer Credentials Presentation Architecture.

The use of DIDs and associated DID documents recorded on the ledger represents the primary and fundamental standard enabling the realization of SSI. The second major standard is a Decentralized Key Management System (DKMS), which enables the use of different wallets across multiple devices without any vendor lock-in. Additionally, the third key standard, DID Auth, is used for authentication over a DID connection. Finally, VCs enable a user to use different wallets on different devices and still have access to their credentials. VCs are interoperable, meaning they can be shared and verified across different systems and platforms, without the need for a centralized authority or intermediaries.

2.3 *Comparison of Identity Systems*

Centralized identity systems rely on a single authority or organization to manage and control user identities. This approach is commonly used in traditional systems where a central server stores the user data and handles authentication. However, this centralized control raises concerns about privacy, as the authority has the potential to track user activity and make changes to their identity without their consent. Users have limited visibility and control over how their personal information is accessed, used, and shared by the central authority. They must trust the central entity to handle their data responsibly and protect it from unauthorized access. Moreover, a breach of the central server can result in the unauthorized access, manipulation, or theft of a vast amount of sensitive user information. Additionally, if the central server of a centralized identity system experiences downtime or encounters technical issues, it can lead to significant service disruptions. Users may find themselves unable to access their accounts or utilize services that require authentication. Lastly, the cease of operation of a centralized authority can result in a complete breakdown of services and a loss of access to

accounts and potentially all associated information, leaving individuals and organizations without means of authentication or access to their digital identities.

Federated identity systems link a person's digital identity and attributes stored across multiple distinct identity management systems. This approach enables single sign-on (SSO) functionality, where a user's authentication token is trusted across multiple domains. SSO is a subset of federated identity management and focuses on technical interoperability for authentication. It streamlines user authentication by enabling access to multiple services with a single set of credentials. Specifically, users authenticate with their preferred IDP, which acts as a trusted intermediary for accessing various applications or services. However, this approach still introduces privacy and security risks. Firstly, users and service providers rely on the availability and security of the central IDP and if it experiences disruptions or breaches, access to multiple services may be compromised. Additionally, users may still have limited control over the sharing of personal data with participating service providers, thus the problem of data privacy is not resolved.

User-centric identity systems aim to provide a consistent user experience across multiple sign-on interactions, regardless of the systems, organizations, or applications involved. This approach emphasizes putting the user in control of their identity and focuses on providing seamless and user-friendly authentication experiences. However, user-centric systems often rely on centralized IDPs or platforms to facilitate the authentication and management of user identities, thus they inherit a lot of the issues of the aforementioned approaches. Additionally, user-centric systems may face challenges in terms of interoperability with other systems and applications. Different platforms may have varying protocols and standards for identity management, making it difficult for seamless integration and data exchange. This can result in a fragmented user experience and additional complexities for organizations seeking to adopt user-centric approaches across their services.

SSI takes the user-centric approach to the next level by giving individuals complete control over their digital identities. SSI allows users to securely store their identity information and use interoperable protocols to present their identity when needed. It aims to prevent identity sharing, provides mechanisms for revocation and recovery, and ensures that users have the ultimate authority over their identity. Specifically, it minimizes personal data exposure by enabling selective disclosure of only necessary information. Additionally, it enables users to hold their cryptographic keys, reducing the risk of centralized data breaches and unauthorized access. It is significant to note that there are trade-offs to adopting SSI. Widespread adoption of SSI requires collaboration and standardization across organizations and industries. Similarly, from the users' point of view, implementing SSI requires infrastructure setup, integration, and technical expertise.

2.4 *Decentralized Identifiers*

DIDs have emerged as a fundamental component of SSI systems, providing a decentralized, secure and interoperable way to represent and manage digital identities. The origins of DIDs can be traced back to the W3C community [36], which recognized the need for a decentralized, standardized way to manage digital identities. In this section, we will explore the fundamentals of DIDs, including their structure and purpose, the role of DID Resolution in enabling interoperability and the concept of DID Auth.

From a high-level perspective, a DID is a new type of identifier that is used to uniquely identify a subject in a decentralized system. These systems provide a secure and transparent means of storing data that can be accessed by anyone with permission. Unlike a Uniform Resource Locator (URL) used on the Internet, a DID can be used to identify a subject in any decentralized network. When querying a conventional URL, the corresponding webpage is returned. In contrast to standard Web links, DIDs possess four notable characteristics: global uniqueness, queryability, high availability and cryptographic verification of data authenticity, making them insusceptible to cyberattacks.

The content retrieved from a DID is cryptographically authenticated, providing a high degree of certainty regarding its authenticity. In addition, a user has the ability to possess and manage multiple DIDs and prove ownership of them by associating them with a public key and governing access to them through a private key. Users create unique cryptographic key pairs that are meant to be used only between the two parties: the user and the entity they shared their DID with. Thus, each user is able to create a lifetime encrypted private channel with the entity they shared their DID with.

Through the use of a DID document, individuals can determine how much information is made public, when and to whom information is shared, as well as the preferred methods of communication. The DID document serves as an expression of these preferences, allowing for greater control and privacy in online interactions. DIDs can be registered directly on a public or private blockchain or a distributed network. This

decentralized ownership and control makes DIDs truly self-sovereign. Using these private channels, users can leverage VCs to establish higher levels of trust.

According to Drummond Reed [37], the format for DIDs was based on the URN RFC 2141, a standard for persistent identifiers on the Internet, authored by Ryan Moats in 1997 [38]. Persistent identifiers are signed and unchanging, thus the aforementioned format was ideal for DIDs, since they need to be persistent and unique so that they can always represent the same entity.

DIDs have a three-part form, with the method identifier allowing different ones to be designed. A simple example of a DID, provided by the recent W3C Recommendation on DIDs [39], is depicted in Figure 4. The first part, "did:," represents that it is a decentralized identifier. The second part is the DID method, such as "sov" for Sovereign, "btcr" for Bitcoin, and "eth" for Ethereum. The third part is a DID method specific identifier, which is the network-specific identifier that uniquely identifies the DID. As is evident, the identifier is non-human-readable, but it is crucial for cryptographic verification and contains all the necessary information for it when resolved to a DID document. Therefore, a DID can be represented as "did:network:identifier" or "did:did-method:did-method-specific-identifier."

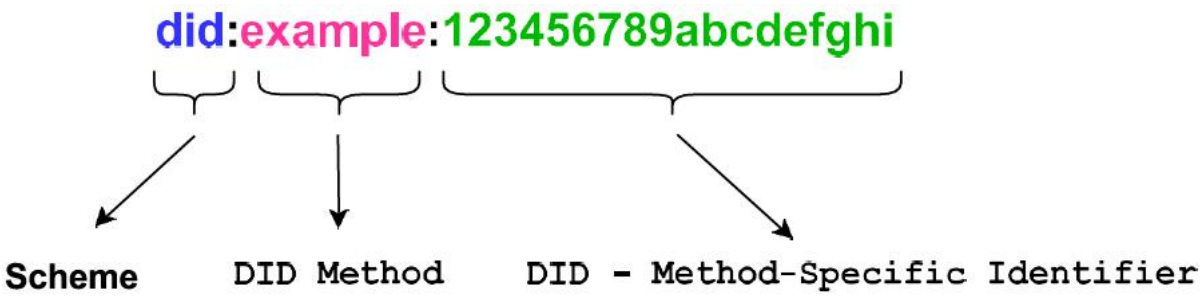

Figure 4. Example of a DID from the recent W3C Recommendation on Decentralized Identifiers (DIDs) [39].

A state-of-the-art technology stack that uses DIDs is Trust over IP (ToIP), which aims to establish trust between peers over digital networks, such as the Internet, by employing a decentralized architecture. It consists of four layers that serve specific purposes [40]. ToIP utilizes DIDs to create decentralized trust roots at layer one, eliminating the need for a central authority and giving users greater control over their personal information. The DIDComm protocol at layer two facilitates secure communication between peers without relying on any particular transport. At layer three, ToIP employs a credential exchange protocol based on the W3C VC standard to enable decentralized and secure issuance and verification of VCs. Layer four adds a metamodel for describing the business, legal, and technical policies under which a peer operates as an issuer, holder, or verifier of digital credentials, which enables the integration of cryptographically verifiable governance frameworks.

2.4.1 DID Methods

A DID method specification is required to define the operations for creating, resolving, updating, and deactivating DIDs. Specifically, the specification must describe how authorization is performed for all operations, including any necessary cryptographic processes. Additionally, it must specify how a DID controller creates a DID and its associated DID document, how a DID resolver uses a DID to resolve a DID document while ensuring the authenticity of the response, and the conditions required for updating a DID document. Finally, the specification must outline the process for deactivating a DID or indicating that deactivation is not possible.

Some of the notable DID methods that are currently in use are displayed in Table 2. While we will provide a brief overview of did:btcr, did:ethr, and did:sov, Fdhila et al. [41] offer a comprehensive analysis and comparison of various DID methods. Furthermore, we will provide an overview of did:self, in accordance with the did:self method specification [42].

Table 2. DID Methods and their DID Prefixes.

Method	DID Prefix	Description
Bitcoin	did:btcr	Uses public-permissionless blockchain
Ethereum	did:ethr	Account-based model and support for smart contracts
Sovrin	did:sov	Permissioned with state proofs
Hyperledger Indy	did:indy	Open-source and uses public-permissioned blockchain
VeresOne	did:v1	Permisionless and blockchain-agnostic
EBSI	did:ebsi	Permissioned and uses Ethereum
Web	did:web	Uses a Web server as registry
Self	did:self	No secure registry required (no blockchain or server)

The DID method DID:btcr employs Bitcoin blockchain transactions for identity registration, updating, and revocation. Due to the public accessibility and permissionless nature of the Bitcoin blockchain, there are no requirements for permission to operate DID:btcr, as anyone can participate in transacting with the ledger. Nonetheless, resolving a DID without relying on authoritative intermediaries mandates the operation of a full Bitcoin node, which can pose difficulties in directly resolving DIDs. Overall, even though using Bitcoin transactions as DIDs guarantees integrity and persistence, referring to continuation documents raises concerns about censorship and mutability.

The did:ethr method is similar to did:btcr in that it builds upon a blockchain technology, specifically Ethereum, which employs an account-based model and supports quasi-Turing complete smart contracts. In contrast to Bitcoin, creating a DID in did:ethr does not require submitting a transaction to the Ethereum network. Any externally owned account address is mapped to an identity. The underlying Ethereum blockchain system provides the network and registry, with the registry governed by a smart contract that can be publicly interacted with through any Ethereum account or other smart contract. An advantage of the did:ethr method is that it allows the creation of a DID without the need for permission or special hardware requirements. Additionally, updates to a DID in the did:ethr registry are publicly visible, which could potentially result in privacy issues. Finally, this method allows for the use of "service endpoints" that can reference external, mutable resources like URLs, which can raise concerns over censorship, persistence, and privacy.

In did:sov, the network and registry both correspond to the Sovrin network. In contrast to did:btcr, writing to the Sovrin ledger is permissioned and restricted to transaction endorsers or nodes, while anyone can read from the ledger. Additionally, DID resolution in did:sov does not require the implementation of a full node, instead it relies on state proofs. Registering a DID without intermediaries is not feasible since it must be carried out through an endorser. Overall, did:sov has been designed to be censorship-resistant by leveraging a decentralized network of nodes located globally.

The did:self method allows for the management of DID documents without relying on registries. A did:self identifier is the thumbprint of a JSON Web Key (JWK) and its corresponding DID document is protected by a JSON Web Signature (JWS) proof generated by the private key that corresponds to the did:self identifier. The public key itself is associated with the DID document, which is then signed by the corresponding private key. This provides a high level of control and ownership over the DID document, which enables a more decentralized and self-sovereign approach to identity management. By using JWK thumbprints and JWS, the integrity and authenticity of DID documents are ensured, which is crucial for secure digital identity management.

Enabling interoperability with multiple DID methods is often a crucial requirement for applications and services. To achieve this goal, such applications and services may leverage DID Resolvers, which can effectively resolve any type of DID data regardless of the underlying DID method. There are several projects and initiatives in the dID space that are developing their own DID Resolver implementations, with the most notable being the Universal Resolver, which has been created and developed by the Decentralized Identity Foundation (DIF) [43].

2.4.2 DID Auth

According to Sabadello et al. [44], the definition of DID Auth pertains to a procedure in which an individual, with the aid of diverse components such as Web browsers, mobile devices, and other agents, provides evidence to a relying party that they possess control over a DID. In essence, this entails the demonstration of control over the DID by the user that owns it.

The DID Auth interaction may be either one-way or two-way, with mutual proof of control of DIDs in the latter case. In order to perform DID Auth, it is necessary to possess the authentication material generated during DID Record creation; a combination of the DID itself and its corresponding DID Document. DID Auth employs a challenge-response process where a relying party verifies the DID of an identity owner. Following the challenge, the identity owner creates a response to demonstrate control over their DID, typically using a cryptographic signature or other forms of proof mechanisms. The response may also include the VCs requested by the relying party in the challenge. The relying party then validates the response by resolving the identity owner's DID and verifying its validity against the prior challenge, such as verifying the response signature with the public key object specified in the DID Document. They can also choose to incorporate the DID Auth interaction into a higher-layer interaction, such as the exchange of VCs, for a specific transaction purpose.

In accordance with the whitepaper by Sabadello et al. [44], the relationship between DID Auth and VCs can be interpreted in one of three ways;

1. The processes of DID Auth and exchange of VCs are distinct from each other. At the beginning of an interaction between two parties, they need to authenticate. Once authentication is successful, a protocol for the exchange of VCs may be executed to enable the two parties to acquire further information about each other.
2. The exchange of VCs is an extension to DID Auth. This entails a single protocol for proving control of an identifier and proving possession of VCs, with the latter being an optional field in the protocol.
3. DID Auth is a type of VC. In this case, DID Auth represents the most basic form of self-issued VC, indicating "I am me."

2.5 *Verifiable Credentials*

SSI systems enable the creation of VCs; digital documents where asymmetric cryptography can be used in order to verify the authenticity of a set of claims regarding a Subject. They are a digital version of traditional documents such as passports, driver's licenses, and certificates. A major difference with traditional documents is that VCs can be securely shared with third parties in order to be verified.

VCs are based on a set of standards defined by the W3C VC Data Model and Encoding as described in [45]. The VC data model defines how an entity's attributes should be structured and encoded in order to be considered a verifiable credential. Due to this structure, there exists a standard, which can be easily verified, so as to ensure the authenticity of the claims contained in the credentials. Moreover, VCs have several benefits compared to physical (identity) documents. For instance, they can be securely shared with multiple parties, while eliminating the need to provide physical documents and exchanging the same information multiple times. Additionally, VCs can be updated and revoked in real-time, ensuring that information remains accurate.

As depicted in Figure 5, a typical VC ecosystem consists of the following entities: the Issuer, the Holder and the Verifier. Initially, the Issuer creates a VC and then transmits it to the Holder. After receiving the VC, the Holder can generate a Verifiable Presentation (VP), which consists of one or more VCs signed by the Holder. It is also possible for the Holder to selectively disclose the attributes she wants to present to a Verifier. Finally, the Verifier receives the VP by the Holder and cryptographically validates its authenticity. Note that in most cases, the Holder of the VC is the Subject upon which claims are made, but sometimes the Holder can be different from the Subject (e.g., a parent can hold the VCs of a child).

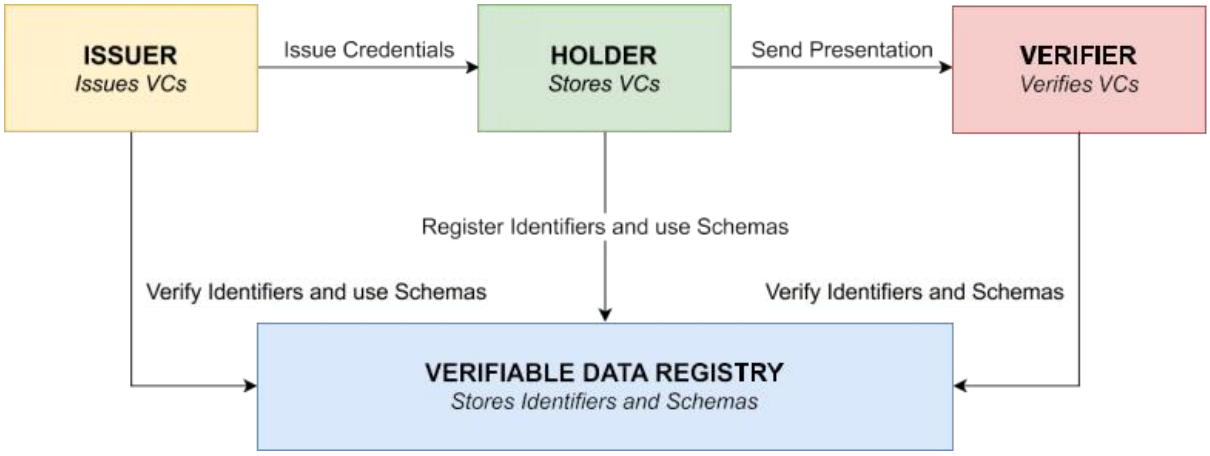

Figure 5. A typical VC ecosystem

The aforementioned operations are supported by a Verifiable Data Registry (VDR), which is responsible for storing the status of the VCs, the revocation registries, the issuer public keys and other information that may be needed from the entities of the system [46]. Typical examples of VDRs are centralized databases and blockchains.

Based on the W3C standard [45], a VC includes several components, some of which are listed below:

- Subject: the entity upon which claims are made. Typical examples of a subject include a person, an organization, and IoT devices.
- Issuer: the entity which assigns the credential that corresponds to the claims of a Subject.
- Claim: statements which refer to a Subject, assigned by the Issuer. Examples of claims include name, address, date of birth, employment history, and other qualifications. Note that a claim is equivalent to a statement. A VC can be described as a set of Verifiable Claims, although in the literature, a credential can be differentiated from claims [47].
- Evidence: additional information that supports the claims of a Subject. For instance, in a driver's license credential, the claim could refer to the fact that a person is authorized to drive, while the evidence could be a photo of the Subject.
- Signature: the VC is digitally signed by the Issuer. In this way the authenticity of the credential and the integrity of the information are ensured.
- Encoding: VCs are encoded in a standard format, such as JSON-LD, to ensure interoperability and secure exchange of information. The encoding of a VC refers to the structure of its components.

Furthermore, it is possible to use a DID URI as the Subject of a VC. In this way, the VC can be linked to a specific DID, which represents the entity and thus a secure and decentralized way to verify the identity of the subject is provided. The DID URI, which refers to the Subject is typically included in the "id" field of the VC and can be used to look up the corresponding DID document, which contains the public key(s) and other metadata needed to verify the authenticity of the credential.

2.5.1 Selective Disclosure

Selective disclosure is an important feature of VCs and VPs as it enables individuals to share only the necessary information with a Verifier, while the rest of their personal data is kept private. This is especially useful in situations where sensitive information is involved, such as when proving a user's identity or providing proof of his age.

If the proofs are created using traditional digital signature schemes, the Holder should present all the attributes that are included in the VC. Therefore, anyone can have access to these attributes, which can lead to potential privacy issues. Moreover, in terms of usability, not all attributes are useful to a Verifier. Due to these facts, cryptographic protocols have been created to enable selective disclosure [48–50].

In Selective disclosure protocols, the Holder chooses the messages she wants to disclose to the Verifier from a list of messages. However, VCs have a structure which is based on standards such as JSON-LD. To enable selective disclosure, it is important to transform these formats into lists of messages. This involves canonicalization algorithms. A privacy-preserving scheme for selective disclosure of VCs using canonicalization algorithms is explained in [51]. Selective disclosure can be assisted with the use of ZKPs [52], by creating a proof about the specific information that the Holder selected to present to a third party. ZKPs are used for selective disclosure as they allow a prover to prove a statement is true without revealing any additional information beyond the truth of the statement [46].

Instead of implementing selective disclosure as previously mentioned, another option is to use separate credentials for each attribute that needs to be disclosed. This approach is discussed in [53]. In this paper, each credential contains only the information that is needed for a specific purpose or use case. For example, if an individual needs to prove their age to purchase alcohol, they would only share a credential that contains their age information, rather than sharing their full identity information. Using separate credentials for each attribute can provide a certain level of privacy, but it is impractical as it will increase the complexity of managing and verifying multiple credentials.

2.5.2 Revocation

Revocation of a credential is required due to theft, loss or change of status, e.g., a student who has completed her studies may no longer be allowed access to the university's infrastructure. When a VC of a Holder is revoked, the verification process should fail and all other entities in the system that need to validate the VC should be informed that its status has changed. We divide revocation mechanisms into three categories:

- Centralized revocation: In this method, a central authority handles the revocation process, typically by maintaining a list of revoked credentials. In this solution, Verifiers check this list before accepting a credential (to determine whether it has been revoked or not). An architecture which is based on this method is Let's Revoke [54]. It is a revocation mechanism that uses Certificate Revocation Vectors (CRVs) in order to store the status of the credentials. The solution is based on dynamically-sized bit vectors, which represent the status of a credential by using a single bit. Each credential has a revocation number, which corresponds to the position of the credential in a particular CRV. If a credential needs to be revoked, the Certificate Authority (CA), who issued the credential, changes the value of the bit of the credential in the CRV from 0 to 1. A similar approach is proposed in a W3C draft [55].
- Decentralized revocation: This method reduces the need for a central authority to maintain information about the revoked credentials. Examples of decentralized revocation are lists stored in the blockchain or solutions that leverage smart contracts. Some decentralized revocation mechanisms include the following. Xu et al. [56] use a blockchain to store legitimate users, disallowing access to illegal users. If a user's public key is not stored in the blockchain, then this user is considered to be illegal and the corresponding credentials have been revoked. The transactions in a block form a Merkle tree in which the first layer is a chameleon hash, which is useful as network operators can alter transactions while keeping the header unchanged. Cerberus [57] consists of the following parts: a university, a student, an employer and the accreditation body that maintains a permissioned blockchain network. Accreditation bodies verify and validate academic credentials issued by universities. In this paper, accreditation bodies are also responsible for setting up and updating Cerberus. The university issues certificates to students, while also digitally signing a transaction that contains the details of the certificates it issues. The transaction is then propagated to the Cerberus network, where it is verified by the accreditation body and finally added to a block. On the other hand, the physical credential contains a QR code, which is used for verification. Veramo [58], which was previously named uPort, uses a single Ethereum smart contract to store the revoked credentials. Users of this system manage their credentials through a mobile application. uPort leverages the Interplanetary File System (IPFS), which provides decentralized storage used to store DID documents. Chotkan et al. [59] propose a gossip-based protocol in order to propagate the revocations through a P2P network. Stokking et al. [60] introduce an SSI system that uses direct P2P communication. They propose three revocation mechanisms for their system: a revocation registry handled by the Issuer, the use of blockchain technology and short validity terms.
- Zero-knowledge proof-based revocation: In this method, a verifier can check the validity of a credential without revealing any additional information about a Subject besides what is necessary. Dynamic accumulators [61] are an example of such systems, as they allow for efficient verification of a set of values without revealing any information about the individual values in the set. More specifically, dynamic accumulators combine a set of values into a single accumulated value. This value is then published or distributed to other parties, who can use it to efficiently check if a particular value is a member of the set without needing to know any of the other values in the set. As a result, dynamic accumulators are considered a private mechanism for revocation of credentials. Typical examples of SSI systems that leverage dynamic accumulators are IRMA (https://irma.app/docs/what-is-irma) and Sovrin [62].

Regardless of the method used, the aim of the revocation mechanism is to ensure that information contained in VCs remains accurate. Most revocation mechanisms that are proposed in existing SSI systems introduce centralized authorities to handle revocations or leverage blockchains or Distributed Ledger Technologies (DLTs) to store information related to the revoked credentials.

Obviously, we can eliminate the need for a revocation mechanism altogether if the validity time of credentials is extremely short, forcing essentially the Holder to request from the Issuer a new VC for every use (presentation). However, this approach goes against the key principle of SSI, where the Holder should be in control. It also introduces potential privacy concerns, but most importantly usability and performance issues, requiring the Issuer to be online and responsive all the time.

2.6 *European Blockchain Services Infrastructure*

The European Blockchain Services Infrastructure (EBSI) [63] is a notable initiative of the European Commission established a secure and trusted infrastructure for cross-border digital public services using blockchain technology. EBSI offers Core Technical Services, including APIs, Smart Contracts, and the EBSI ledger, that are hosted in a decentralized manner across Europe by a network of nodes. With the goal of promoting efficiency and trust in digital transactions, EBSI enables the development of innovative digital solutions that can improve public services.

Decentralized Identifiers In accordance with the EBSI DID method specification [64], two distinct DID Methods have been implemented to cater to Legal Entities (LE) and Natural Persons (NP). The DID Method for Legal Entities entails that the Legal Entity DIDs are public identifiers and are guaranteed to be unique through the DID Registry. On the other hand, the DID Method for Natural Persons focuses on pseudonymous identifiers to ensure the privacy of the individual. This method does not mandate the registration of any DID, DID Document, or public keys. In the EBSI context, a specific Schema is defined as follows;

did:ebsi:<method-specific-identifier>.

Verifiable Credentials and Verifiable Presentations Another key feature of EBSI is its support for VCs and VPs, which are essential components of its ecosystem, as they allow for the secure sharing and verification of digital identities, attributes, and qualifications across different organizations and borders. The VC and VP data models used in EBSI are based on the W3C VCs [65], which establish the standardized method for presenting certificates and credentials digitally on the Internet. The integrity and reliability of the data and credentials are established through the utilization of digital signatures and various cryptographic techniques. To facilitate secure online transactions in the European Single Market (ESM), the Electronic Identification, Authentication and Trust Services (eIDAS) regulation has laid down standards for electronic signatures. A significant aspect of eIDAS pertains to the establishment of a uniform system for electronic identification (eID) and trust services that includes electronic signatures, seals, time stamps, and delivery services. This standardization enables citizens and enterprises to utilize their respective national eIDs to access services offered in other EU member states, thereby minimizing the requirement for multiple identification credentials. EBSI is fully compliant with the eIDAS Regulation and is ensuring adherence to its stipulations [66], as it provides a legal and regulatory framework for electronic identification and trust services.

Use Cases EBSI's functional capabilities are grouped into several families, including Verifiable Credentials, Trusted Data Exchange, and Track and Trace, each of which is further subdivided into specific domains, where EBSI can be utilized to support the creation of cross-border services [67]. The Track and Trace Use Case Family currently offers options for document traceability and Small and Medium-sized Enterprises (SMEs) Financing. The primary focus of this family is to provide a reliable, secure, and decentralized system for tracking the movement of documents and eventually goods throughout supply chains. This helps to increase transparency, reduce the risk of fraud and counterfeiting, and improve efficiency in supply chain management. All VCs are based on a self-sovereign information sharing pattern where the holders of credentials have control over how, when, and by whom their information is verified, using an EBSI Conformant wallet. Upon selecting the document traceability option, users should be presented with a system illustrated in the architectural diagram in Figure 6.

To elaborate on this use case, we will consider a hypothetical scenario where a company is required to comply with various regulations and standards, such as ISO 9001 or ISO 14001, in order to operate in a certain industry. To demonstrate compliance, the company must maintain various documents, such as quality manuals, procedures, and audit reports. However, these documents can be susceptible to fraud, alteration, or loss, which can result in severe legal and financial consequences for the company. Thus, the company can use a document traceability system based on blockchain technology, such as EBSI. This scenario is illustrated in Figure 6, where four actors are involved: the Holder, represented by the company that needs to demonstrate compliance with the regulations and standards, the Verifier, represented by a regulatory body or a customer who wants to ensure that the company is compliant with the necessary regulations and standards, the Issuer, represented by the company itself or a third-party auditor that verifies the company's compliance and issues a verifiable attestation or certificate, and the Accrediting Body, represented by a regulatory agency that oversees the industry in which the company operates. When a document is created, in order to ensure its credibility, the company creates a digital signature, which is verified by the Issuer and is recorded on the EBSI ledger. Later, when changes or updates are made to the document, they are also recorded on the ledger, along with the date and time the event occurred, the identity of the person who made the change, and cryptographic proof of the change. When the Verifier audits the company's compliance, they can use the EBSI system to verify the authenticity and integrity of the documents. Or, in other words, the verifier queries the EBSI Ledger. Additionally, the utilization of EBSI allows verifiers to view the entire history of each document, including its origin, movement, and any changes made to it. This helps to ensure that the company is in full compliance with industry regulations and standards and avoids any legal or financial consequences that may result from non-compliance. During the creation and updates of documents, the verifiable data is transmitted to the Accrediting Body, which then registers the cryptographic proofs of the data onto the EBSI Ledger, enabling various Verifiers to utilize them accordingly.

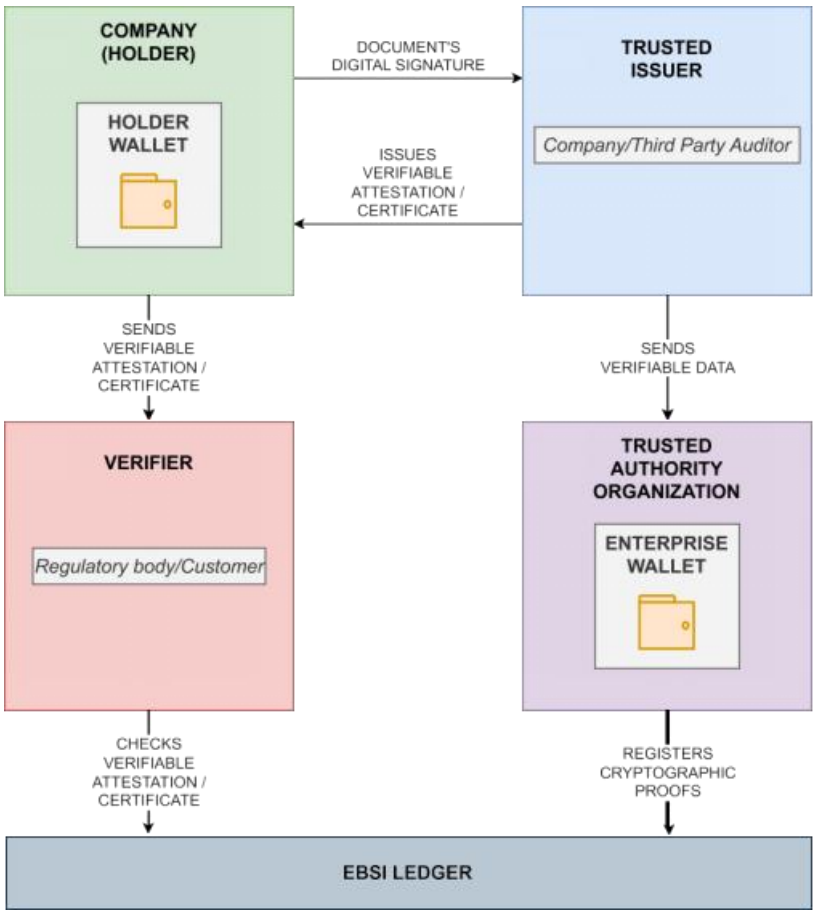

Figure 6. EBSI Track and Trace family Use Case example.

The **Digital Product Passport** (DPP) aims to enhance the circularity and sustainability of products by providing a novel approach to support the transition towards a circular and low-carbon economy. Specifically, the DPP is a standardized digital record or documentation intended to provide details on a product's origin, composition, repair and dismantling options, as well as information on how it should be handled at the end of its lifecycle. By providing comprehensive data on a product's environmental and social impact, quality, safety, and origin, the DPP enhances supply chain transparency, traceability, and accountability. The supply chain is a multifaceted system that encompasses all entities, resources, and processes involved in producing and delivering a product or service, including sourcing, procurement, logistics, transportation, and distribution [68]. The European Union is committed to promoting sustainability and has implemented several policies and regulations under the European Green Deal (EGD) to achieve net-zero emissions by 2050 [69]. By integrating DPP into EBSI, a secure and trustworthy platform can be created to manage and exchange product information within the EU. Berg et al. [69] provide a use case example for implementing an ecosystem that enables trusted electronic product information management for plastic products' lifecycle. Although this example is specific to the plastics industry, the overall design can be applied to all products. With the involvement of blockchain in the digital product passport and the requirement for trust, the adoption of SSI solutions becomes necessary. The key design goals for this ecosystem, along with the approaches to achieving them are the following:

- Control: The authors suggest using SSI to enable direct control over product information by the manufacturer.
- Decentralization: The utilization of DIDs is proposed to create a unique identifier for every company in the supply chain and every product or material.
- Interoperability and Extensibility: The utilization of DIDs and VCs standardized by the W3C is proposed, enabling anyone who implements those standards to participate in the decentralized ecosystem.
- Portability and Resolvability: DIDs and VCs linked to a product identity can be represented as QR Codes, which helps to transfer them from the digital to the physical world.
- Security: Access control mechanisms can be implemented to grant access through VCs only to authorized applications and users.

European Digital Identity Wallets are electronic means of securely storing and managing personal data, electronic or digital identities, and credentials for users. These wallets are crucial to accessing cross-border services facilitated by EBSI and managing digital credentials. Consistent with this objective, the European governments provide citizens with electronic identities in the form of government eID credentials, containing digital certificates that enable them to demonstrate their identity with a significant level of certainty in various public or private services. Furthermore, the eIDAS Regulation supports mutual cross-border recognition of government eIDs, and European Union countries voluntarily prompt their eID schemes to the European Commission, which assesses their compliance with eIDAS criteria [70]. DIGITALEUROPE is a prominent trade association that represents industries undergoing digital transformation within Europe. Their primary objective is to support a reform of the eIDAS Regulation, which seeks to establish a stronger framework for electronic identification and trust services [71]. Specifically, DIGITALEUROPE proposes specific changes to the final text of the regulation to guarantee an effective revision, such as prolonging issuance and implementation timeframes, allowing different methods to implement high security, and aligning electronic identification language with existing legislation. Additionally, DIGITALEUROPE acknowledges the importance of European digital wallets, which include the EU Digital Identity **(**EUDI) Wallet, in enabling secure and user-friendly access to cross-border services while prioritizing personal data protection and privacy through trusted eID schemes.

Web 3.0 and EBSI's Decentralized Trust Model Web 3.0, also referred to as the decentralized Web, is a fundamental design blueprint that concentrates on creating protocols and underlying technologies that enable secure, *decentralized* information exchange. EBSI aims to offer the elements of a Web 3.0 trust model by combining three fundamental technologies that ensure secure and reliable information exchange [72]. These technologies include VCs, Digital Wallets, and a Blockchain Ledger, all of which are designed to enable trusted, decentralized environments for information exchange while ensuring data privacy and security. By incorporating these technologies, EBSI provides a secure, decentralized platform for information exchange, which is a vital step toward the realization of Web 3.0.

3. Decentralized Identity Applications for the IoT

3.1 *The Internet of Things*

The IoT is a network that consists of physical devices, such as vehicles, home appliances, and other "things" with embedded sensors and software, connected such that the exchange of data is enabled. The aim of IoT devices is to perform automated tasks without human intervention. The idea behind IoT is mostly incentivized by low-cost sensors, wireless networks, and Cloud computing technologies, which have made it possible to collect and analyze vast amounts of data from any type of device or environment. There is a wide range of potential IoT applications, which include smart homes, smart cities, industrial automation, environmental monitoring, and automation and new capabilities in healthcare and transportation.

The concept of the IoT was first proposed by Kevin Ashton in 1999 [73]. Although there is no official definition of the IoT that is universally accepted, there exist several organizations that have proposed their own definitions. For instance, the International Telecommunication Union (ITU) defines IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [74]. The European Research Cluster on Internet of Things (IERC) defines IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [75]. These definitions highlight the important parts of the IoT environment, such as connectivity, interoperability, and the ability to exchange data between devices. Note that an important aspect of the IoT is the actuation capability, allowing the cyber world to have an impact on the real, physical world, and thus raising the security and safety stakes, typically also leading to robustness and auditing requirements and raising the importance of identity, authentication, authorization and access control.

We will analyze the characteristics that enable IoT devices to collect, transmit, and process data from a wide range of sources and environments, making the IoT ecosystem useful for a broad range of applications and use cases in various domains and industries. Initially, all IoT devices are connected to the Internet or other networks, in order to communicate with other devices and exchange data. Sensors are also a crucial component of IoT devices as they enable them to detect changes in their environment and perform actions in response to

those changes. Many IoT devices are designed to operate on low power, allowing them to run for extended periods on a single battery or other power source. Additionally, processors and memory are included in many IoT devices, so as to analyze data locally, without the need for constant communication with servers. Finally, each IoT device must have a unique identifier or address that distinguishes it from other devices in the network. Due to unique identities, devices can be tracked and managed properly.

In the field of IoT, various architecture models are being proposed and followed, as evidenced by the existing literature. As presented by the Sovrin Foundation [8], one of these models is a simple three-layer architecture model for IoT systems. It consists of a Wireless Sensor Network (WSN), a Cloud server layer, and a business application layer. Incorporating SSI into this architecture model for the IoT would introduce several changes. While the WSN layer would remain responsible for collecting sensor data, SSI would provide an additional layer of security to ensure that this data can only be accessed by authorized parties. In the Cloud server layer, SSI could be used to authenticate and authorize access to data stored in the Cloud, as well as to facilitate secure data transfer between the WSN and the Cloud. Finally, the business application layer could implement identity management and access control mechanisms, thus reducing the risk of unauthorized access to sensitive data and services. Overall, the addition of SSI to the architecture model would help to address some of the critical security and privacy concerns associated with the IoT, such as data privacy, authentication, and access control.

3.2 *Applications of SSI in the IoT*

Various applications and frameworks have been proposed in an attempt to incorporate SSI principles to improve identity management, by providing total control over the identity of device owners. In this section, we mention some of these architectures by discussing their contributions in order to highlight the benefits of using SSI in an IoT ecosystem.

Lagutin et al. [76] recognize the potential of utilizing SSI for enhancing security in IoT environments. However, they acknowledge that implementing SSI in systems with constrained IoT devices can be challenging due to management and resource limitations. Therefore, they introduce an approach that involves delegating the processing of DIDs and VCs from constrained IoT devices to the OAuth Authorization Server by extending the Authentication and Authorization for Constrained Environments (ACE) - OAuth flow. This approach has been implemented as an open-source software under the SOFIE project [77]. This method significantly expands the number of devices that can utilize DIDs and VCs. Additionally, they propose a solution for local authentication, which was not addressed by ACE-OAuth. Finally, the paper evaluates the resulting improvements and suggests opportunities for further protocol optimization.

In [4], a new method for securing 5G IoT device registration and software update is proposed. The authors argue that current methods used for this purpose introduce centralization and thus are vulnerable to several attacks. They leverage DIDs and more specifically the Microsoft ION DID method in order to enhance the system's security, while also storing DIDs in public blockchains to achieve scalability and decentralization. The proposed system, called Gnomon, allows IoT devices to register themselves with the network using their DID and a set of public keys. The network then verifies the device's identity using the DID and if it is authenticated correctly, it is allowed to connect to the network. Software updates are also handled similarly. Once an update is available, the network sends a message to the device with its DID, which initially verifies the message and subsequently checks the authenticity of the update in order to finally install it. The authors conducted experiments to test the effectiveness of Gnomon and concluded that it provides a more secure and efficient method for device registration and software updates regarding 5G IoT devices.

Mahalle et al. [78] also argue that the current methods for managing identities and credentials in IoT environments are centralized, insecure, and often incompatible with other systems. To address these issues, the authors propose a new framework for IoT ecosystems that utilizes the use of DIDs and VCs. The proposed framework allows IoT devices to generate their own DIDs and use them to securely authenticate themselves with other devices and services. VCs can then be used to verify the device's identity and claims about its capabilities, such as the type of sensors it has or the data it can provide.

Another study which was proposed by [79] aimed to address the challenges regarding security and identity management in IoT devices. This work leverages DLTs and SSI in order to grant total ownership and control over users' identities. More specifically, it enables device registration, generation of a unique identifier and creation and assertion of VCs, which correspond to claims regarding a Subject. Also, it utilizes a trust score algorithm which is based on the WoT for IoT devices, while introducing a risk mitigation and management mechanism so as to enhance the overall security of the system and minimize the consequences that may occur as a result of vulnerabilities during manufacture, or other attacks. Finally, the aforementioned mechanism informs

a revocation authority to revoke the credentials of a device based on the trust score algorithm when it is necessary. The proposed solution is scalable, interoperable, portable and offers a certain level of security.

The authors in [5] also use DIDs and the WoT in order to implement an identity management framework for IoT devices. Similarly, identities are managed through DIDs, which are stored in the blockchain, while security and scalability are also achieved through trusted ratings in the WoT. The authors proved that their system is resilient to certain attacks, while also addressing issues regarding identity and trust. They also note that their system can be easily integrated into existing solutions and thus achieving scalability. For future work, they argue that they will enhance privacy by leveraging ZKPs on constrained devices.

The DIAM-IoT Framework [10] is an access management framework for IoT devices that incorporates VCs and DIDs in its architecture. Through the utilization of DIDs and VCs, a global identity is created, managed, and controlled by IoT device owners, who can then easily share their data with other devices. Also, the framework itself includes DIDs and VCs in the IoT device lifecycle, resulting in minimizing the work needed for device manufacturers. User-centric access control is enabled in the DIAM-IoT framework as it enables users to create customized rules for granting access requests to their device information, which gives them complete authority over their data. Finally, transparency is achieved using smart contracts, which record the transactions between device owners and requesters. The authors prove these properties by creating a decentralized data authorization proof-of-concept, which demonstrates the potential of their architecture. The same authors have also implemented the DIAM-IoT framework with a Pebble tracker [80], which is a GPS tracking device with 4G connectivity and sensors. By designing their proof of concept, they show that their system successfully manages access requests and enforces data authorization policies in a decentralized and secure manner. Overall, their framework offers a promising approach to addressing the growing need for decentralized and secure IoT data authorization systems.

Jung [6] aims to address the challenge of implementing access control in the IoT in order to achieve scalability and solve the issues that centralized systems introduce. The benefits of the proposed model include decentralization, which is achieved through DIDs, usability as it separates the profiles of users and devices and versatility as the model's differentiated membership can be adapted to various IoT use cases. However, the author acknowledges that the model is in early stages and needs to be improved in terms of privacy and security in order to avoid unauthorized users altering DID documents.

Moreover, in [81] Liu et al. propose a capability-based IoT access control policy, which leverages blockchain and DIDs. They implemented their system and the experiments showed that it is scalable and secure exploiting a permissioned blockchain, where a group of organizations come together to form a decentralized network for the purpose of sharing data and conducting transactions. Also, they evaluate the system in terms of security and they demonstrate that it achieves confidentiality, enforces authorized access and supports revocation. They ensure data integrity and immutability, while their system also provides timely recovery thanks to storing local replicas of all transaction history, which can be used for recovery. Although their system provides several advantages, it is suitable only for a consortium blockchain network. Nevertheless, the authors plan to re-design their system for a public blockchain, while also incorporating token propagation in IoT devices.

De Diego et al. [82] leverage SSI in order to create an IoT-as-a-service (IoTaaS) business model. In particular, the authors highlight the importance of IoTaaS as a model that offers IoT devices on demand, which results in lower costs, optimized use of resources and the ability to reuse an IoT device. There are a few challenges that this model introduces, but the study focuses on the identity problem. The authors utilize SSI principles in order to enable total control over users' identities in a model in which devices are offered on demand. They use VCs and DIDs as defined by the corresponding W3C standards to manage identity in the IoT device life-cycle. The proposed system introduces a marketplace, meaning an interface which connects device owners with devices, which also can be viewed as a storage for VPs. More specifically, since the VCs are not stored in the marketplace, devices have the ability to control the information they send to the marketplace through VPs. ZKPs can be used to generate these VPs, thereby ensuring privacy when necessary. It's important to note that the marketplace cannot generate ZKPs because it does not hold the original VCs; instead, only devices can generate them. In this way, the marketplace can act as a proxy for VPs containing these ZKPs. However, the authors acknowledge the tradeoff between privacy and performance since the use of ZKPs could improve device privacy but could also require devices to answer queries and verification requests from consumers, while at the same time constructing ZKPs, which could impact performance. Finally, in the performance evaluation, the authors tested their solution in terms of creation, exchange and verification of VPs and the results indicated that the average time needed to complete these actions does not limit the system's performance and thus incorporating SSI solutions into their architecture is suitable.

Furthermore, Cocco et al. [7] propose a decentralized architecture which is based on Veramo in order to manage data related to buildings, such as construction and maintenance information, blueprints and building

management. This solution manages all data regarding both stakeholders and IoT devices, which are placed in the buildings. In particular, stakeholders and buildings are identified by DIDs, while IoT devices are represented as delegates of buildings. The entities of the system can easily manage their own identities, while also selectively disclosing the attributes they want to show to a third party using ZKPs. Additionally, entities of the system can interact with each other through the Information Management Platform, which includes user interfaces, Ethereum smart contracts and servers. The overall solution offers privacy as it leverages ZKPs to share VCs, transparency as it is based on the Ethereum infrastructure and traceability as IoT devices can be easily tracked thanks to their representation as delegates of buildings. Finally, by utilizing SSI and IoT principles, the model aims to transform the construction industry, leading to decreased costs, less time and lower complexity. In addition, these technologies can help bridge the gap between citizens and institutions, building trust in digital services and making them more widely available.

Fotiou et al. [83] address security challenges in IoT systems with one-to-many and many-to-one communication patterns and propose a solution using DIDs and VCs to address the provenance verification security challenge in CoAP group communication. CoAP is a lightweight protocol designed for the IoT, with resources identified by URIs and a client-server model similar to HTTP. Each CoAP group is associated with a DID and VCs are used to assert IoT endpoint membership in the group. The DID method that is utilized in the proposed system is did:self [42] since it provides several relevant benefits, as presented earlier. Briefly, this DID method allows for the inclusion of any type of information in the DID document without limitations or specific registry requirements. Additionally, the responsibility for disseminating DID documents lies with the owners of did:self DIDs, providing flexibility in how the documents are shared. Moreover, did:self ensures the accuracy of the DID document even when retrieved over an unsecured channel. Finally, the ability for multiple valid DID documents to coexist for a specific did:self DID allows for each IoT device to be configured with a distinct DID document of the same did:self DID belonging to the device owner. The proposed solution allows easy addition or removal of IoT endpoints to/from a CoAP group and easy detection of breached signing keys.

Finally, Zeydan et al. [84] propose a novel method for vehicular networks, which leverages SSI concepts and blockchain technology. A vehicular network is a type of communication network where vehicles, road infrastructure, and other mobile devices are interconnected to exchange information. Vehicular networks allow vehicles to communicate with each other, with the surrounding infrastructure, and with the Internet, forming a complex network of connected devices that can share real-time data such as traffic conditions, road hazards, and weather information. Clearly, vehicular networks are a subset of the IoT ecosystem. The authors aim to address the challenge of confidentiality and integrity of user data that blockchain-based SSI solutions introduce. Initially, confidentiality is enabled by preventing unauthorized access to the transactions of permissioned blockchain networks, by using SSI principles in order to grant access only to authorized users. In addition, integrity is achieved by utilizing permissioned blockchains for information related to the vehicular network, while authorization is enabled through the link between the SSI-blockchain permissionless network and the blockchain permissioned network.

4. Benefits and Challenges of SSI for the IoT

4.1 *Benefits*

Incorporating SSI technology into IoT systems offers several advantages identified and categorized by Fedrecheski et al. [2]:

- Owner-Centric designs: SSI technology can facilitate the creation of owner-centric IoT environments. Users will have the ability to create identities that they own, control and manage, which will enable the easy establishment of a network of devices that belong to them. Although these devices will maintain their individual identities within the IoT system, the utilization of SSI will transform the formation of trust relationships within the system, as devices with the same owner will immediately trust each other.
- Privacy-Preserving: IoT systems that incorporate SSI technology will aid in the protection of users' privacy. In conventional IoT systems, users' personal information would be stored in a Service Provider (SP). By incorporating SSI, sensitive data will be stored in digital wallets and the backup process will entail encryption, with the user holding exclusive ownership of the decryption keys. Moreover, users will possess the ability to choose the individuals or entities with whom they will share their credentials, and potentially utilize techniques such as selective disclosure, ZKP, and so on to further enhance privacy.
- Decentralized operation: One of the prominent benefits of integrating SSI technology in IoT systems is decentralization. In addition to transferring control of personal data from centralized authorities to

individuals, which enables them to manage their data without relying on intermediaries, the utilization of SSI also enables users to determine when their identity ceases to be valid, and it gives them a similar level of control over their devices. As a result, users are no longer reliant on SP, which could potentially make them vulnerable to single points of failure.

- End-to-end security: Another advantage is the establishment of secure communications between two endpoints. Specifically, by exchanging DID documents and using asymmetric cryptography, IoT systems can perform mutual authentication (DID Auth), derive short-lived symmetric keys, transmit encrypted messages, and more. This approach can be applied independently of transport protocols, which enables secure communication even between devices that use different communication protocols.
- Layered authentication: The incorporation of SSI technologies in IoT environments, leads to the distinction of cryptographic authentication from application-specific authentication. This separation will ensure that endpoints are always cryptographically protected, while higher-level trust requirements will be managed at the application layer. Cryptographic authentication will involve the mutual proof of possession of specific public keys between two devices, whereas application-specific authentication will involve the proof of different attributes about the devices.
- Interoperability and robustness: Finally, the utilization of SSI technology in IoT systems, allows for the development of interoperable solutions. This is due to the fact that VCs and DIDs are developed by W3C as open specifications and JSON is utilized by both SSI and IoT systems. Additionally, EBSI's interoperability efforts can facilitate the integration of various IoT devices and systems, enabling them to function seamlessly and securely.

Integrating SSI technology into IoT systems can also enable them to accomplish some of their own objectives and requirements, such as:

- Data Minimization: SSI technology has a significant role to play in achieving the general objective of data minimization in IoT systems. The principle of data minimization states that IoT devices should collect and process only the necessary data required to serve their intended purpose. SSI technology can facilitate this by enabling users to share only the minimum amount of data required for a specific use case instead of having to disclose their entire identity or data profile. The technology allows for selective disclosure of credentials, giving users the ability to choose which credentials to share with whom and for how long.
- Consent and Control: SSI can aid in achieving the objective of Consent and Control in the IoT, which involves providing users with proper information regarding the control and consent over the collection, utilization, and sharing of data by IoT devices. This approach enables users to provide informed consent for the collection, utilization, and sharing of their data by IoT devices. Additionally, SSI allows users to revoke access to their data at any time, giving them more control over their data.
- Anonymization: The utilization of SSI in IoT systems can aid in achieving the goal of Anonymization. SSI allows for the use of VCs, enabling the selective disclosure of information without revealing any unnecessary personal data. This means that users can choose to disclose only the information that is essential for a specific use case while keeping their full identity concealed.
- Data Subject Rights: In IoT systems, it is important for users to have the right to access, rectify, or delete their personal data. SSI technology can help IoT fulfill this goal by providing users with complete control over their personal data and the ability to selectively share their data using VCs. This allows users to easily access, rectify, or delete their personal data stored on IoT devices as needed. With SSI, users can exercise their data subject rights more easily and effectively in IoT environments, which enhances their privacy and data protection.
- Data Retention: SSI technology can assist IoT environments in achieving the objective of Data Retention, which involves retaining sensitive data on IoT devices and networks only for the necessary amount of time to achieve their intended purpose. With SSI, users have the ability to control their personal data completely and selectively disclose them. This allows users to reduce the amount of personal data stored on IoT devices and networks and establish expiration dates for their data.

4.2 *Challenges*

Despite the several benefits that SSI introduces for IoT environments, there are still some challenges that need to be handled before adopting an SSI architecture in an IoT ecosystem. Most of these challenges are a result of the features of IoT devices, which may introduce limitations to the design of the ecosystem:

- Constraints of IoT devices: In order to incorporate an SSI architecture in an IoT environment, it is essential that devices use public key cryptography, which may be a challenge for devices with low processing power.

Furthermore, IoT devices should also be able to exchange VCs and DID documents. This is especially difficult when IoT devices are highly constrained and may not even be able to connect to the Internet to have access to a DID document if it is not stored locally. However, Lagutin et al. [76] address the challenge of implementing SSI in systems with constrained IoT devices by proposing to delegate the processing of DIDs and VCs to OAuth Authorization Servers, by extending the ACE-OAuth flow.

- Communication: The size of DID documents and VCs may result in communication overhead if the packet size of the communication protocol is not large enough. In order to overcome this limitation, compression, fragmentation, and infrequent transmission of documents may be necessary [2].
- Security: IoT devices are often vulnerable to cyber-attacks [3], and because of that, SSI systems should be designed according to IoT device constraints in order to protect user data and prevent unauthorized access to devices. In the next sections, we will analyze how SSI systems can contribute to the security of an IoT ecosystem.
- Scalability: SSI systems may not able to handle the vast amount of data which is generated by IoT devices. Hence, a system that incorporates an SSI architecture into an IoT ecosystem may not be scalable enough. However, as previously mentioned, existing implementations provide solutions to address this issue. For instance, Gnomon [4] utilized public blockchains for storing DIDs and the authors in [5] used trusted ratings in the WoT, in order to achieve scalability.
- Usability: In SSI systems users should manage their own credentials, which may result in poor user experience. Due to that, IoT devices should provide a simple and friendly user interface that will help users to effectively handle their credentials. However, there are existing solutions which improve usability, such as [6], where user profiles are separated from IoT devices, resulting in a simpler and easier way to manage identities. Also, in [7], usability is addressed by providing friendly user interfaces, which allow third parties to verify subject claims.

5. SSI Contributions to Security and Privacy in the IoT

5.1 *Contributions to Privacy*

The IoT is rapidly evolving, with billions of interconnected devices and systems enabling new levels of efficiency, productivity and convenience. However, its mostly unattended operation, mostly low cost devices, its pervasiveness in the environment with often potential easy physical and wireless proximity access by attackers, and finally its sheer massiveness, pose significant challenges to privacy and security. To be precise, the collection, processing, and sharing of personal data by IoT devices can create significant privacy risks, particularly when this data is used without the knowledge or consent of users. As IoT devices become more interconnected, the potential for privacy violations and data breaches also increases. This highlights the importance of implementing strong privacy protections for IoT devices, so as to ensure the minimization of privacy and security risks.

Extensive research has been conducted in the area of privacy for the IoT [9, 85–88]. Enhanced privacy can be achieved by incorporating SSI systems in the IoT ecosystem. In this section, we will provide a detailed analysis of how SSI systems can help IoT devices manage their data in a secure and decentralized manner. The following are the main contributions of SSI to IoT device privacy:

- Identification: Each IoT device must have a unique identifier which distinguishes it from other devices. SSI systems are particularly useful in this case, as they provide a global way to possess, prove and share a user's identity. By leveraging DIDs and VCs, the system ensures that devices will be securely identified and authenticated and this will be independent of networking technologies, location etc.
- Consent and Control: In an IoT system, users should consent and have control over the use and exchange of data that are being shared by their IoT devices. Thanks to decentralization, SSI systems allow users to have total control over their personal data without having to rely on any intermediaries. Therefore, SSI solutions require that users consent to sharing their data with or from IoT devices, while also choosing with whom to share this data.
- Secure and authorized exchange of data: Due to selective disclosure and ZKPs, SSI systems allow the Holder of a credential to present only the minimum information required to a third party. Disclosing only the necessary data requires the use of cryptographic protocols which ensure data privacy and integrity. Therefore, IoT devices will be able to securely exchange information with other devices, while also avoiding unauthorized access. VCs can also be revoked and thus when a device should no longer have

access to a resource or when it is compromised, the permission to use this resource can be easily denied. ZKPs and selective disclosure are used in several papers [7, 79, 82]. In these systems, device owners are able to select the attributes they will disclose to the Verifier, while no additional data is required for the verification process. Alternative solutions to achieve authorized exchange of data, without selective disclosure and ZKPs could be through the utilization of OAuth, as presented by Fotiou et al. [21], FIDO and VCs which are leveraged by Chadwick et al. [23], and OpenID Connect, which is based on the OAuth 2.0 framework and allows for the use of VCs.

- Data ownership: Moreover, VCs have been implemented in a way that the Holder of the credential could differ from the Subject, meaning for instance that a parent can hold the VCs of their child. Hence, a user can grant access to their IoT devices to another user in a privacy preserving manner.
- Device control [8]: DIDs can be implemented such that they will be suitable even for constrained devices with a variety of characteristics. Even if a device has limited capabilities, it can be enhanced with the use of agents and wallets. Moreover, managing users and devices in an SSI system increases efficiency, as it removes the burden to set up and configure devices and users' rights. When a device connects to the network, it can generate its identity with the use of DIDs. DIDs enable rotation and revocation and thus can be used efficiently and securely, limiting the use of a central authority to manage identifiers and enhancing privacy. Proposed systems such as Gnomon [4] and the system presented by the authors in [81] demonstrated their efficiency through experiments.

5.2 *Contributions to Security*

With the rapid growth of the IoT, the security of connected devices has emerged as a major challenge. With the transmission and storage of sensitive personal data, it is essential to ensure that IoT systems are secure from potential threats. SSI technology offers a promising solution to address some of the security challenges faced by IoT systems. SSI provides a decentralized and secure way to manage identities and personal data, which can help protect the privacy and security of IoT users. In this section, we will examine the various ways in which SSI can contribute to IoT device security.

Alhirabi et al. [87] and Tawalbeh et al. [85] identify some of the major security risks and requirements associated with IoT systems. Some contributions of SSI to IoT environments in regard to security, also brought up by the Sovrin Foundation [8], are the following:

- Access control: Through the issuance of VCs that specify access privileges, SSI allows users to control who can access data on IoT devices, thereby mitigating the risk of data breaches arising from unauthorized access. The DIAM-IoT Framework [10] enables user-centric access control as users can create customized rules for granting access requests to their IoT device data. Liu et al. [81] propose a capability-based IoT access control policy, which utilizes a consortium blockchain network and DIDs.
- dID management: By employing SSI's decentralized approach to identity management, IoT systems can avoid relying on a single point (of potential failure, or attack target), thus decreasing the likelihood of cyberattacks that may endanger sensitive data stored on IoT devices.
- Tamper-evident data: SSI technology allows the use of tamper-evident VCs, which can detect any unauthorized changes made to the data stored on IoT devices. This ensures the integrity of the data and helps to prevent attacks such as data tampering or injection, which could compromise the security of the IoT system.
- Secure communication: Through the use of VCs, SSI technology enables IoT devices to authenticate each other, thus ensuring secure communication and mitigating the risk of data interception or tampering by unauthorized parties.
- Scalability: Traditional centralized identity management systems can become overwhelmed and cause scalability issues as the number of IoT devices increases. However, with SSI, there is no central authority or database, which allows for a more distributed and scalable approach to identity management. In addition, SSI can enable interoperability between different IoT devices and platforms, which can reduce the complexity of managing identity and access control for different devices. As we previously mentioned, several systems propose scalable solutions as [4–6, 79, 81].
- Movement and transfer of ownership: The movement and transfer of ownership of IoT devices can pose security risks, including unauthorized access, data leakage, and malicious activity. To address these risks, SSI provides a reliable and secure method for transferring ownership through the use of VCs, as they can establish proof of ownership, minimizing the potential for unauthorized access to the device. Furthermore, SSI facilitates the secure transfer of associated data, preserving its confidentiality and integrity during the transfer process.

In conclusion, the adoption of SSI can potentially enhance the security of IoT systems. SSI offers a decentralized approach to identity management and access control, which mitigates the risks of unauthorized access, data breaches, and malicious behavior. SSI also provides tamper-evident data, secure communication, and reliable transfer of ownership, making it beneficial for IoT systems to increase scalability and interoperability. The utilization of VCs enables users to control access to their personal data, reducing the risk of unauthorized data processing and collection. Thus, SSI presents a promising solution for addressing the security and privacy challenges faced by IoT environments.

6. Conclusions

The proliferation of IoT devices has led to an increase in security and privacy concerns, as centralized identity management solutions are not ideal for the highly distributed and heterogeneous nature of IoT networks. dID solutions, such as SSI, have emerged as a promising alternative to conventional identity management approaches. Incorporating SSI into IoT systems would enable devices to manage their own identities independently, reducing the need for intermediaries and centralized authorities. In this paper, we provide a comprehensive analysis of the benefits and challenges that arise from integrating SSI principles into IoT systems. We also explore the potential of dID solutions for enhancing security and privacy in IoT environments. Incorporating SSI technology into IoT systems offers a variety of benefits, ranging from enhanced security and privacy, to decentralization, refined flexibility and agility, and even more improved interoperability. SSI technology enables users to create and control their own identities, allowing them to form dynamic trust relationships easily, particularly among IoT devices with the same owner or in the context of groups of users with complex relationships, e.g., in an enterprise environment. Additionally, SSI allows users to retain full control of personal data, thus empowering them to manage their data without relying on centralized third-party services or applications and eliminating reliance on single points of failure. SSI also enables establishing secure communications between IoT devices through the utilization of DID Auth and asymmetric cryptography. Moreover, SSI separates cryptographic authentication from application-specific authentication, ensuring endpoints are always cryptographically protected and higher-level trust requirements are managed at the application layer. Finally, SSI facilitates interoperability and robustness in IoT systems by utilizing standardized specifications for VCs and DIDs, and thus utilizing JSON in both SSI and IoT systems.

As vast amounts of data are being gathered and shared by IoT devices, privacy risks are escalating. Therefore, it is important that secure mechanisms are implemented so as to minimize the risk of unauthorized access to sensitive information. SSI attempts to solve the aforementioned issue by introducing a way for identifying users and devices that leverages DIDs. By utilizing SSI principles, users have total control over their personal data and can selectively disclose their information with the use of ZKPs, which enhances privacy. In addition, IoT systems can make use of protocols such as OAuth, FIDO and OpenId for the same purposes. There are even efficient SSI-based solutions for IoT constrained devices, which is a concern in many IoT architectures as they have limited process capability. Moreover, by enabling a secure revocation mechanism for such a system, privacy can be further enhanced as credentials will be revoked without revealing any personal information to third parties.

SSI technology can provide a promising solution to the security challenges faced by IoT systems by offering a decentralized and formal way to manage identities and personal data, protecting the privacy and security of IoT users and data. Specifically, SSI enables access control to IoT devices through the issuance of VCs. Additionally, as SSI offers a decentralized approach to identity management, it reduces the risk of cyberattacks. Tamper-evident VCs allow for detecting any unauthorized changes made to the data stored on IoT devices. Furthermore, SSI technology enables IoT devices to authenticate each other, ensuring secure communication. SSI also offers a scalable approach to identity management and enables interoperability between different IoT devices and platforms. Finally, SSI provides a secure method for transferring ownership of IoT devices and associated data through the use of VCs.

In spite of the several advantages that the incorporation of SSI principles in the IoT ecosystem introduces, there are still some open challenges that need to be addressed. Initially, a common issue is related to the communication overhead as the size of VCs and DID documents may be larger than corresponding data in more traditional approaches and may not match the packet size of the network, particularly for IoT systems. There may be some solutions to this problem, but this remains a challenge. Another open issue is related to high cost and complexity. Further experimentation is required in order to evaluate the performance of such systems and to create architectures with reasonable cost and lower complexity. Revocation mechanisms also remain a technical challenge in SSI systems, as most systems use central authorities to handle revoked credentials, violating

decentralization. While ZKP based revocation may be a privacy-preserving solution, efficiency is an issue. Therefore, the revocation mechanism to be used in an IoT ecosystem that leverages SSI solutions needs to be carefully designed in order to balance privacy with efficiency. The aforementioned trade-off is also present in IoT systems that incorporate SSI principles in general, as privacy enhancing solutions are often less efficient.

While there are challenges to integrating SSI technology into IoT environments, the substantial benefits and contributions to privacy and security justify the pursuit of this initiative. Therefore, it is imperative to address the open challenges, in order to encourage the widespread adoption of SSI in IoT systems. It is also worth noting that this is an emerging area of research and development and advances in technology and standards and collaboration among stakeholders can help overcome the challenges. With the continued efforts to improve the integration of SSI technology into IoT systems, we can look forward to a future where individuals have greater control over their personal data and data in IoT environments in general.

Conflict of Interest

There is no conflict of interest for this study.

References

[1] Siwakoti, Y.R.; Bhurtel, M.; Rawat, D.B.; Oest, A; Johnson, R.C. Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures. *IEEE Internet Things J.* **2023**, *10*, 11224–11239, http://dx.doi.org/10.1109/JIOT.2023.3252594.

[2] Fedrecheski, G.; Rabaey, J.M.; Costa, L.C.; Ccori, P.C.C.; Pereira, W.T.; Zuffo, M. K. Self-Sovereign Identity for IoT environments: A Perspective. *arXiv preprint* arXiv:2012.02444, https://doi.org/10.48550/arXiv.2003.05106.

[3] Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices, *IEEE Internet Things J.* **2019**, *6*, 8182–8201, https://doi.org/10.1109/JIOT.2019.2935189.

[4] Ansey, R.; Kempf, J.; Berzin, O.; Xi, C.; Sheikh, I. Gnomon: Decentralized identifiers for securing 5g IoT device registration and software update. In Proceedings of 2019 IEEE Globecom Workshops, Waikoloa, Hawaii, USA, 9–13 December 2019, pp. 1–6, https://doi.org/10.1109/GCWkshps45667.2019.9024702.

[5] Luecking, M.; Fries, C.; Lamberti, R.; Stork, W. Decentralized Identity and Trust Management Framework for Internet of Things. In Proceedings of 2020 IEEE International Conference on Blockchain and Cryptocurrency, Toronto, On, Canada, 3–6 May 2020, pp. 1–9, https://doi.org/10.1109/ICBC48266.2020.9169411.

[6] Jung, E. A Decentralized Access Control Model for IoT with DID. In Proceedings of 8th International Conference on IT Convergence and Security, Online, 19–21 August 2020, pp. 141–148, https://doi.org/10.1007/978-981-16-4118-3.

[7] Cocco, L.; Tonelli, R.; Marchesi, M.; A System Proposal for Information Management in Building Sector Based on BIM, SSI, IoT and Blockchain. *Future Internet* **2022**, *14*, 140, https://doi.org/10.3390/fi14050140.

[8] Self-Sovereign Identity and IoT. Available online: https://sovrin.org/wp-content/uploads/SSI-in-IoT-whitepaper_Sovrin-design.pdf (accessed on 5 March 2023).

[9] Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44, https://doi.org/10.3390/info7030044.

[10] Fan, X.; Chai, Q.; Xu, L.; Guo, D. Diam-iot: A Decentralized Identity and Access Management Framework for Internet of Things. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Online, 5–9 October 2020, pp. 186–191, https://doi.org/10.1145/3384943.3409436.

[11] The path to Self-Sovereign Identity. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereereign-identity.html (accessed on 24 March 2023).

[12] Internet Assigned Numbers Authority (IANA). Available online: https://www.ietf.org/standards/iana/ (accessed on 24 March 2023).

[13] Internet Corporation for Assigned Names and Numbers (ICANN). Available online: https://www.icann.org/ (accessed on 24 March 2023).

[14] Certificate authority. Available online: https://www.techtarget.com/searchsecurity/definition/certificate-authority (accessed on 24 March 2023).

[15] Caronni, G. Walking the Web of Trust. In Proceedings of IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Gaithersburg, Maryland, USA, 14–16 March 2000, https://doi.org/10.1109/ENABL.2000.883720.

[16] Motykowski, P. An Analysis of User-Centric Identity Technology Trends, Openid's First Act, MSc Thesis, Regis University, Denver, Colorado, USA, 2011.
[17] Jordon, K.; Hauser, J.; Foster, S. The Augmented Social Network: Building identity and trust into the next-generation Internet. *First Monday*, **2003**, *8*, 8, http://dx.doi.org/10.5210/fm.v8i8.1068.
[18] Kahrs, M.; Nguyen, K. Future ecosystems for secure authentication and identification. In Proceedings of ISSE 2015 Highlights of the Information Security Solutions Europe 2015 Conference, Rome, Italy, 28–30 September 2015, http://dx.doi.org/10.1007/978-3-658-10934-9_2.
[19] RFC 6749 - The OAuth 2.0 Authorization Framework. Available online: https://datatracker.ietf.org/doc/html/rfc6749 (accessed on 24 March 2023).
[20] RFC 5849 - The OAuth 1.0 Protocol. Available online: https://datatracker.ietf.org/doc/html/rfc5849 (accessed on 24 March 2023).
[21] Fotiou, N.; Faltaka, E.; Kalos, V.; Kefala, A.; Pittaras, I.; Siris, V.; Polyzos, G. Continuous authorization over HTTP using Verifiable Credentials and OAuth 2.0. Open Identity Summit 2022, LNI Volume P325 Complete, pp. 39-50, https://doi.org/10.18420/OID2022_03.
[22] FIDO Specifications. Available online: https://fidoalliance.org/specifications/download/ (accessed on 30 April 2023).
[23] Chadwick, D. W.; Laborde, R.; Oglaza, A.; Venant, R.; Wazan, S.; Nijjar, M. Improved Identity Management with Verifiable Credentials and FIDO. In Proceedings of the 2nd International Conference on Identity, Security, and Behavior Analysis, London, England, 27 February 2020, pp. 14–20, https://doi.org/10.1109/MCOMSTD.001.1900020.
[24] OpenID Authentication 1.1. Available online: https://openid.net/specs/openid-authentication-1_1.html (accessed on 24 March 2023)
[25] Avellaneda, O.; Bachmann, A.; Barbir, A.; Brenan, J.; Dingle, P.; Duffy, K. H.; Maler, E.; Reed, D.; Sporny, M. Decentralized identity: Where did it come from and where is it going? *IEEE Commun. Stand. Mag.* **2019**, *3*, 10–13, https://doi.org/10.1109/MCOMSTD.2019.9031542.
[26] OpenID Authentication 2.0 – Final. Available online: https://openid.net/specs/openid-authentication-2_0.html (accessed on 5 March 2023).
[27] Openid Connect Core 1.0 incorporating errata set 1. Available online: https://openid.net/specs/openid-connect-core-1_0.html (accessed on 5 March 2023)
[28] Openid for Verifiable Credentials – Overview. Available online: https://openid.net/sg/openid4vc/ (accessed on 5 March 2023)
[29] What is 'sovereign source authority'? Available online: http://www.moxytongue.com/2012/02/ what-is-sovereign-source-authority.html (accessed on 23 March 2023).
[30] Self-Sovereign Identity. Available online: http://www.moxytongue.com/2016/02/self-sovereign-identity.html (accessed on 24 March 2023).
[31] The respect trust network v2.1. Available online: http://oixnet.org/wp-content/uploads/2016/02/ respect-trust-framework-v2-1.pdf (accessed on 24 March 2023).
[32] Identity System Essentials. Available online: https://www.evernym.com/wp-content/uploads/2017/02/Identity-System-Essentials.pdf (accessed on 24 March 2023).
[33] The world citizen: Transforming statelessness into global citizenship. Available online: http://blogs.worldbank.org/ic4d/category/tags/self-sovereign-identity-systems (accessed on 23 March 2023).
[34] Web of Trust - Self Sovereign Identity. Available online: https://github.com/WebOfTrustInfo/self-sovereign-identity (accessed on 24 March 2023).
[35] The inevitable rise of self-sovereign identity. Available online: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (accessed on 23 March 2023).
[36] W3C community. Available online: https://www.w3.org/community/ (accessed on 24 March 2023).
[37] Decentralized identifiers (DIDs): The Fundamental Building Block of Self-Sovereign Identity – Drummond Reed – Webinar 2. Available online: https://ssimeetup.org/decentralized-identifiers-did-fundamental-block-self-sovereign-identity-drummond-reed-webinar-2/ (accessed on 25 March 2023)
[38] RFC 2141 - URN Syntax IETF. Available online: https://datatracker.ietf.org/doc/html/rfc2141 (accessed on 25 March 2023).
[39] Decentralized Identifiers (DIDs) v1.0. Available online: https://www.w3.org/TR/did-core/ (accessed on 25 March 2023)
[40] Davie, M.; Gisolfi, D.; Hardman, D.; Jordan, J.; O'Donnell, D.; Reed, D. The Trust over IP Stack. *IEEE Commun. Stand. Mag.* **2020**, *3*, 46–51, https://doi.org/10.1109/MCOMSTD.001.1900029.
[41] Fdhila, W.; Stifter, N.; Kostal, K.; Saglam, C.; Sabadello, M. Methods for Decentralized Identities: Evaluation and insights. In Proceedings of Business Process Management: Blockchain and Robotic Process

Automation Forum, Rome, Italy, 6–10 September 2021, pp. 119–135, https://doi.org/10.1007/978-3-030-85867-4_9.
[42] DID Self Method Specification. Available online: https://github.com/excid-io/did-self (accessed on 24 March 2023).
[43] Decentralized identity foundation. Available online: https://identity.foundation/ (accessed on 25 March 2023).
[44] Introduction to DID Auth. Available online: https://nbviewer.org/github/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf (accessed on 25 March 2023).
[45] Verifiable Credentials Data Model 1.0. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 25 March 2023).
[46] Soltani, R.; Nguyen, U.T.; An, A. A Survey of Self-Sovereign Identity Ecosystem. *Secur. Commun. Networks 2021*, *2021*, 1–26, https://doi.org/10.1155/2021/8873429.
[47] 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, https://doi.org/10.1016/j.cosrev.2018.10.002.
[48] Bauer, D.; Blough, D. M.; Cash, D. Minimal information disclosure with efficiently verifiable credentials. In Proceedings of the 4th ACM workshop on Digital identity management, Virginia, USA, 31 October 2008, pp. 15–24, https://doi.org/10.1145/1456424.1456428.
[49] Camenisch, J.; Van Herreweghen, E. Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002, pp. 21–30, https://doi.org/10.1145/586110.586114.
[50] U-Prove Cryptographic Specification v1.1 revision 3. Available online: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Cryptographic20Specification20V1.1.pdf (accessed on 25 March 2023).
[51] Kalos, V.; Polyzos, G. C. Requirements and secure serialization for selective disclosure verifiable credentials. In Proceedings of the ICT Systems Security and Privacy Protection 2, Copenhagen, Denmark, 13–15 June 2022, pp. 231–247, https://doi.org/10.1007/978-3-031-06975-8_14.
[52] Fiege, U.; Fiat, A.; Shamir, A. Zero Knowledge Proofs of Identity. *J. Cryptol.* **1988**, *1*, 77–94, https://doi.org/10.1007/BF02351717.
[53] The Laws of Identity. Available online: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed on 25 March 2023).
[54] Smith, T.; Dickinson, L.; Seamons, K. Let's revoke: Scalable global certificate revocation. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, San Diego, California, 23–26 February 2020, http://dx.doi.org/10.14722/ndss.2020.24084.
[55] Revocation list 2020: a privacy-preserving mechanism for revoking verifiable credentials. Available online: https://w3c-ccg. github.io/vc-status-rl-2020/ (accessed on 25 March 2023).
[56] Xu, J.; Xue, K.; Tian, H.; Hong, J.; Wei, D. S.; Hong, P. An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks, *IEEE Trans. Veh. Technol.* **2020**, *69*, 6688–6698, https://doi.org/10.1109/TVT.2020.2986041.
[57] Tariq, A.; Haq, H. B.; Ali, S. T. Cerberus: A Blockchain-based Accreditation and Degree Verification System. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1503–1514, https://doi.org/10.1109/TCSS.2022.3188453.
[58] uPort: A Platform for Self-Sovereign Identity. Available online: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf (accessed on 25 March 2023).
[59] Chotkan, R.; Decouchant, J.; Pouwelse, J. Distributed Attestation Revocation in Self-Sovereign Identity. In Proceedings of the 47th Conference on Local Computer Networks, Edmonton, Canada, 26–29 September 2022, pp. 414–421, https://doi.org/10.48550/arXiv.2208.05339.
[60] Stokkink, Q.; Ishmaev, G.; Epema, D.; Pouwelse, J. A Truly Self-Sovereign Identity System. In Proceedings of the 46th Conference on Local Computer Networks (LCN), Online, 4–7 October 2021, pp. 1–8, https://doi.org/10.48550/arXiv.2007.00415.
[61] Camenisch, J.; Lysyanskaya, A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Procceedings of the Advances in Cryptology, Santa Barbara, California, USA, 18–22 August 2002, pp. 61–76, https://doi.org/10.1007/3-540-45708-9_5.
[62] Sovrin: digital identities in the blockchain era. Available online: https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf (accessed on 24 March 2023).
[63] European Blockchain Services Infrastructure. Available online: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure (accessed on 24 March 2023).
[64] EBSI DID Method. Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+DID+Method (accessed: 24 March 2023).

[65] Verifiable Credentials Data Model 1.0. Available online: https://w3c.github.io/vc-data-model/WD/2018-07-18/ (accessed on 24 March 2023).
[66] E-signing and e-sealing Verifiable Credentials and Verifiable Presentations. Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/E-signing+and+e-sealing+Verifiable+Credentials+and+Verifiable+Presentations (accessed on 24 March 2023).
[67] EBSI Use Cases. Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/use+cases (accessed on 24 March 2023).
[68] Adisorn, T.; Tholen, L.; Götz, T. Towards a digital product passport fit for contributing to a circular economy. *Energies* **2021**, *14*, 2289, https://doi.org/10.3390/en14082289.
[69] Overcoming information asymmetry in the plastics value chain with digital product passports: How decentralised identifiers and verifiable credentials can enable a circular economy for plastics. Available online: https://epub.wupperinst.org/frontdoor/index/index/docId/7940 (accessed on 24 March 2023).
[70] Universal wallets 2020. Available online: https://w3c-ccg.github.io/universal-wallet-interop-spec/ (accessed on 24 March 2023).
[71] Towards more effective and coherent electronic identification in europe. Available online: https://www.digitaleurope.org/resources/towards-more-effective-and-coherent-electronic-identification-in-europe/ (accessed on 24 March 2023).
[72] EBSI Verifiable Credentials. Available online: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Verifiable+Credentials (accessed on 24 March 2023).
[73] Ashton, K. That 'internet of things' thing. *RFID journal* **2009**, *22*, 97–114, https://doi.org/10.4236/jssm.2015.84056.
[74] Overview of the Internet of Things. Available online: https://www.itu.int/rec/T-REC-Y.2060-201206-I (accessed on 24 March 2023).
[75] Vermesan, O.; Friess, P. Internet of things applications-from research and innovation to market deployment, 1st ed.; River Publishers, Aalborg, Denmark 2014; pp. 7–15.
[76] Lagutin, D.; Kortesniemi, Y.; Fotiou, N.; Siris, V. A. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices using OAuth-based Delegation. In Proceedings of DISS 2019 – Workshop on Decentralized IoT Systems and Security, San Diego, California, USA, 24 February 2019, pp. 6–12, http://dx.doi.org/10.14722/diss.2019.23005.
[77] Sofie Project. Available online: https://github.com/SOFIE-project (accessed on 24 March 2023).
[78] Mahalle, P. N.; Shinde, G.; Shafi, P. M. Rethinking Decentralised Identifiers and Verifiable Credentials for the Internet of Things. In the Internet Things, Smart Computing Technology: A roadmap ahead, Day, N.; Mahalle, P. N.; Shafi, P. M.; Kimabahune, V.V.; Hassanien, A. E.; Springer, Midtown Manhtattan, New York City, USA, 2019, pp. 361–374.
[79] Gebresilassie, S. K.; Rafferty, J.; Morrow, P.; Chen, L.; Abu-Tair, M.; Cui, Z. Distributed, Secure, Self-Sovereign Identity for IoT devices. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020, http://dx.doi.org/10.1109/WF-IoT48130.2020.9221144.
[80] Fan, X.; Chai, Q.; Li, Z.; Pan, T. Decentralized IoT Data Authorization with Pebble Tracker. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020, https://doi.org/10.1109/WF-IoT48130.2020.9221130.
[81] Liu, Y.; Lu, Q.; Chen, S.; Qu, Q; O'Connor, H.; Choo, K.-K. R., Zhang, H. Capability-Based IoT Access Control using Blockchain, *Digit. Commun. Networks* **2021**, *7*, 463–469, https://doi.org/10.1016/j.dcan.2020.10.004.
[82] De Diego, S.; Regueiro, C.; Macia-Fernandez, G. Enabling Identity for the IoT-as-a-service Business Model, *IEEE Access* **2021**, *9*, 159965–159975, https://doi.org/10.1109/ACCESS.2021.3131012.
[83] Fotiou, N.; Siris, V. A.; Xylomenos, G.; Polyzos, G.C. IoT Group Membership Management using Decentralized Identifiers and Verifiable Credentials, *Futur. Internet* **2022**, *14*, 173, https://doi.org/10.3390/fi14060173.
[84] Zeydan, E.; Mangues, J.; Arslan, S.; Turk, Y. Blockchain-based Self-Sovereign Identity Solution for Vehicular Networks. In Proceedings of the 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova I la Geltru, Spain, 17–20 April 2023, pp. 1–7, https://doi.org/10.1109/DRCN57075.2023.10108183.
[85] Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions, *Appl. Sci.* **2020**, *10*, 4102, https://doi.org/10.3390/app10124102.

[86] Ukil, A.; Bandyopadhyay, S.; Pal, A. IoT-Privacy: To be private or not to be private. In Proceedings of the 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April 2014–2 May 2014, pp. 123–124, https://doi.org/10.1109/INFCOMW.2014.6849186.
[87] Alhirabi, N.; Rana, O.; Perera, C. Security and Privacy Requirements for the Internet of Things: A survey. *ACM Trans. Internet Things* **2021**, *2*, 1–37, https://doi.org/10.1145/3437537.
[88] Weber, R. H. Internet of Things: Privacy Issues Revisited. *Comput. Law Secur. Rev.* **2015**, *31*, 618–627, http://dx.doi.org/10.1016/j.clsr.2015.07.002.