electronics

MDPI

Article

eID and Self-Sovereign Identity Usage: An Overview

Daniela Pöhn *, Michael Grabatin and Wolfgang Hommel

Research Institute CODE, Universität der Bundeswehr München, 85579 Neubiberg, Germany; michael.grabatin@unibw.de (M.G.); wolfgang.hommel@unibw.de (W.H.)
* Correspondence: daniela.poehn@unibw.de; Tel.: +49-(0)89-6004-7356

Abstract: The COVID-19 pandemic helped countries to increase the use of their mobile eID solutions. These are based on traditional identity management systems, which suffer from weaknesses, such as the reliance on a central entity to provide the identity data and the lack of control of the user over her or his data. The introduction of self-sovereign identity (SSI) for e-government systems can strengthen the privacy of the citizens while enabling identification also for the weakest. To successfully initiate SSI, different factors have to be taken into account. In order to have a clear understanding of the challenges, but also lessons learned, we provide an overview of existing solutions and projects and conducted an analysis of their experiences. Based on a taxonomy, we identified strong points, as well as encountered challenges. The contribution of this paper is threefold: First, we enhanced existing taxonomies based on the literature for further evaluations. Second, we analyzed eID solutions for lessons learned. Third, we evaluated more recently started SSI projects in different states of their lifecycle. This led to a comprehensive discussion of the lessons learned and challenges to address, as well as further findings.

Keywords: identity management; self-sovereign identity; governmental identities; electronic identity; eIDAS

Citation: Pöhn, D.; Grabatin, M.; Hommel, W. eID and Self-Sovereign Identity Usage: An Overview. *Electronics* **2021**, *10*, 2811. https://doi.org/10.3390/electronics10222811

Academic Editor: Diana Berbecaru

Received: 29 October 2021
Accepted: 11 November 2021
Published: 16 November 2021

1. Introduction

With the COVID-19 pandemic, many public and private organizations needed to find ways to continue their service to customers and business partners. As in-person contact was either avoided or even prohibited, digital processes gained importance. In order to authenticate and log into, for example, e-government services, users need reliable digital identities first. One important way to enable critical business processes is the use of national electronic identities (eIDs). In Europe, the regulation on electronic identification and trust services (eIDAS) [1–3] became effective in 2016. It defines a legal framework to harmonize digital identity and trust services in the European Economic Area (EEA), to enable businesses, consumers, and governments to seamlessly communicate in an international context. The lockdown phases of the pandemic have lead to an explosion of online collaborations. Looking at countries such as Italy, a massive uptake of eID and e-government use on a national level [4,5] can be observed. Furthermore, a major revision of eIDAS is on the way, taking the lessons learned and notable paradigm shifts in the field of identity management into account.

So far, the Security Assertion Markup Language (SAML) [6] is widely deployed as a technical basis in, for example, the federations of eIDAS within Europe and the international interfederation for research and education (R&E) eduGAIN [7]. At the same time, the protocols Open Authentication (OAuth) 2.0 [8] and OpenID Connect (OIDC) [9] are applied, primarily for web-based applications and services and made popular in the consumer area by companies such as Google and Amazon. However, these well-established identity management systems suffer from various design-inherent issues, including single points of failure, lack of interoperability, and privacy issues. In more recent years, decentralized and self-sovereign identity (SSI) solutions gained attention in research and practice [10,11].

The term SSI is frequently used for identity management approaches based on distributed ledger technologies. According to Mühle et al. [12], SSI allows users to fully own and manage their digital identity without having to rely on third parties. Thereby, SSI can be seen as a new evolutionary identity model, next to the traditional centralized, federated, and user-centric identity management that evolved earlier in this century [13,14].

In order to launch SSI successfully, the solutions need to reach a significant share through adoption by users who then are able to control their identity data. Yet, users will only adopt if they see a benefit, which has to be provided, e.g., through adoption by several handy online services. As an example, services related to e-government are widely used in Estonia. Tsap et al. [15] described complexity, ease of use, functionality, awareness, trust, privacy, security, control and empowerment, and transparency as success factors for the public acceptance of eID in Estonia.

This paper is dedicated to the research questions: What can be learned from successful, as well as unsuccessful real-world eID and SSI projects, and what should be taken into account when starting new such projects? Our goal is to provide a comprehensive overview including some technical background and derive design recommendations. The rest of this paper is structured as follows: Section 2 introduces the basics of federated identity management and self-sovereign identities before Section 3 summarizes similar previous and related work. We introduce a taxonomy to systematically analyze challenges in Section 4. A broad analysis of traditional eID and emerging SSI projects is presented in Sections 5 and 6, respectively, to identity success factors, as well as current challenges. The findings are discussed in detail in Section 7. Section 8 concludes the paper and gives an outlook on our future work.

2. Background

In order to understand the current identity management ecosystem, its challenges, and new directions, we provide a short overview of the different predominant directions in both research and practice.

2.1. Federated Identity Management

Federated identity management (FIM) allows users to utilize credentials from their home organization, i.e., an identity provider (IDP), to sign into other services within a so-called *federation*. A federation is basically an organizational boundary for a set of IDPs and service providers (SPs) that share a common goal, such as the use of government-issued digital identities for online services. FIM thus enhances the classic centralized identity management, in which users had to register a separate account at each entity, the services of which they wanted to use. Applying FIM, the user only has to remember the credentials, e.g., username and password, needed for her or his IDP. Although this approach has better usability properties than unrelated separate accounts, it comes with several downsides. For example, the impact of identity theft is much higher, and the user's IDP becomes an entity, which might collect data about which users are using which connected services. Two main FIM protocol families have been established: (1) SAML for large-scale federations such as eIDs [16] and R&E [7] and (2) OAuth for web authorization in combination with OpenID Connect for web authentication. Both can apply a level of assurance (LoA) for trust estimation.

2.1.1. Security Assertion Markup Language

The development of SAML started about two decades ago with a second—and so far final—version published seven years later. SAML 2.0 is an open standard for exchanging authentication and authorization data between entities in the eXtensible Markup Language (XML) format. Both eduGAIN and eIDAS are based on SAML. SAML federations are rather static due to the necessary a priori exchange of XML metadata about the technical communication endpoints between a federation's IDPs and SPs. Since the protocol is

comparably old, which does not diminish its success, it is not optimally suited for mobile applications and other more recent developments.

2.1.2. OAuth 2.0 and OpenID Connect

Modern applications often apply application programming interfaces (APIs) to reuse functions and combine different use cases. The user then gives consent that an application is allowed to call the API on her or his behalf to access resources owned by her or him. OAuth 2.0 provides this functionality, whereas OIDC provides authentication on top of it. Considering that the web ecosystem changed since OAuth 2.0 was developed, several extensions have been introduced in order to try to support more modern use cases; while they also can be considered to be very successful, they are making the overall usage more complex as well [17]. As a result, new versions of OAuth and future protocols are currently being developed [18,19].

2.1.3. Level of Assurance

Being defined by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 29115 Standard [20], the level of assurance describes the *degree of confidence* in the processes leading up to and including the authentication. An LoA provides assurance that the entity claiming a particular identity is the entity to which that identity was assigned. Thereby, an LoA refers to, e.g., the following:

- The entity has been adequately verified during credential enrollment by a registration authority or IDP. This process is also called identity proofing;
- The authenticator being used for the authentication process has not been compromised;
- The claim is true and up-to-date;
- The entity owns and controls the claims or credentials they present.

Different LoA specifications exist, including ISO 29115 [20], eIDAS [1], Internet Engineering Task Force (IETF) Request for Change (RFC) 8485 Vectors of Trust [21], and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 [22]. These can be applied within FIM protocols. The verifiable claims (VCs), used in SSI, can be seen as an adequate representative in this context.

2.2. Self-Sovereign Identities

Recent advances and a certain hype around the development of blockchain technology promote the use of completely decentralized systems for identity management processes. SSI is an identity management system that allows users to fully own and manage their digital identities. Blockchain is a subtype of distributed ledger technology (DLT) and shares similar features and characteristics with other types of DLTs. DLTs are replicated and cryptographically secured databases, in addition to the inherent decentralization of blockchains. Decentralized ledgers and blockchains apply different fault-tolerant consensus mechanisms to ensure that the network can agree on one single truth about data states, transactions, and ensure the consistent state of the network without having to trust a single central entity. In the context of identity management, SSIs make the user the ultimate owner of his or her personal data. Thereby, the users exist independently of services. This contrasts previous identity management approaches, where the user heavily relies on either the government, one's workplace, universities, or private companies such as Facebook (Facebook Connect), Google (Google Sign-In), or Apple (Sign in with Apple).

2.2.1. The Concept around SSI

The SSI concept mainly consists of the following elements:

Decentralized identifiers (DID) provide a standard, that enables the identification of entities while specifying flexible retrieval methods for many use cases;

Verifiable credentials are cryptographically signed collections of user attributes;

Digital wallets are the software to store one's own private keys, verifiable credentials, and DID documents;

Digital agents and hubs provide an interface to the user and persistent endpoints—usually offered by third parties—that serve as a proxy for the mobile digital wallets.

Using those primitives, a system is constructed that enables entities—each identified by a DID and further described by its DID document—to interact with each other. The three main roles, of which an entity usually assumes one of, are the verifiable credential *issuer*, *holder*, and *verifier*. First, an issuer produces a verifiable credential for the holder, who stores the credential in her or his digital wallet. During the authentication process, the holder uses the verifiable credentials to generate a verifiable presentation, which is then passed to the verifier. The verifier can then confirm the signatures within the presentation to check the validity of the holder's claim. Notably, this process does not involve the issuer after the VC has been created initially.

2.2.2. Decentralized Identifiers

One fundamental building block of SSI is the decentralized identifiers. Their central position and importance are strengthened by the fact that they have been standardized by the W3C [23]. As a special kind of uniform resource identifier (URI), they provide a way to identify any kind of entity (the DID's subject) and link to the entity's metadata (the DID document). The entity in control of a DID can warrant its control without external permission, inputs, or support.

An exemplary DID looks as follows `did:example:0123456789abcdefgh` and is constructed out of three parts separated by a colon:

- The scheme identifier `did` followed by;
- The DID method (`example`);
- The identifier, which is specific to the selected DID method.

Using the DID, a resolver can obtain the corresponding DID document, which contains the necessary public key so that the entity in control of the DID can authenticate itself as the DID controller.

2.2.3. Current Protocols

The current state of the SSI ecosystem is heavily influenced by the first large proponent of such a system, the Sovrin Foundation [24]. The research and implementation of the Sovrin Foundation were transferred into the Linux Foundation's SSI projects. In the style of the Internet, the SSI stack is also divided into several layers to abstract functionality [25]. Figure 1 shows an SSI stack based on this design.

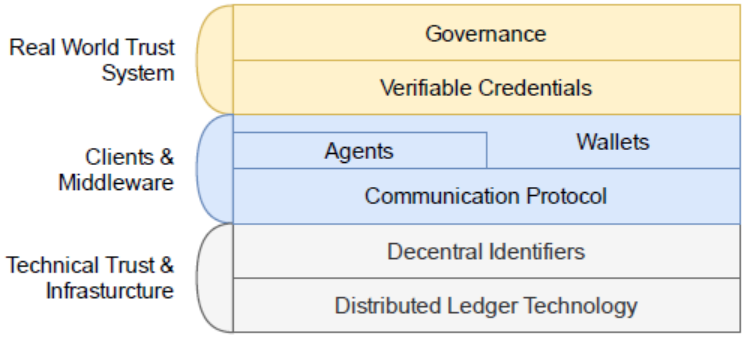

Figure 1. Schematic overview of the SSI stack.

One of the most prominent instances of a fully fledged SSI ecosystem is developed using the projects Hyperledger Indy [26] and Hyperledger Aries [27]. Hyperledger Indy serves as the infrastructure providing technical trust by implementing distributed ledger

technology designed and optimized for identity management. Hyperledger Aries builds on top of Indy and specifies protocols and interfaces for exchanging verifiable credentials, thus bridging the middleware to the real-world trust systems, shown in Figure 1.

3. Previous and Related Work

Several papers specify SSI itself. A NIST whitepaper features a taxonomy for SSI [28], categorizing different blockchain architectures, governance models, and other aspects. Mühle et al. [12] described the essential SSI components identification, authentication, verifiable claims, and storage. Kubach and Sellung [29] analyzed the market of SSI ecosystems and emphasized the need to understand the market, not only the technology. The SSI ecosystem has a specific market structure with network effects and complex trust relationships. The authors also showed the growing number of new SSI projects and wallets, though the market and its offerings are still immature and under development.

3.1. Overview of eID and SSI Solutions

Carretero et al. [30] provided an extensive overview of FIM including software and selected federations. However, the overview of national eID solutions was limited and not up-to-date. Kuperberg et al. [31] reviewed eID and SSI projects worldwide. Yet, since the paper was published, new projects have emerged (e.g., the German showcase program Secure Digital Identities [32]), while others ended (e.g., ZugID in Switzerland [33]).

Further papers concentrated on a single or few selected eID solutions in certain countries [34–36] or their application in specific use cases [37,38]. Deliverable 1.1 of the EU H2020 project mGov4EU [39] provides an overview of the current state of eIDs with a focus on mobile (cross-border) services. Therefore, SSI projects are not regarded, and the focus is preliminary limited.

3.2. SSI Challenges

SSI projects face different challenges. Dib and Toumi [40] categorized those into technical limitations and nontechnical issues. Regarding technical limitations, they stated blockchain as the distributed ledger and key storage. The authors further listed legacy systems, regulations, standards, adoptions, accessibility, and the behaviors of actors as nontechnical issues. In contrast, Kubach et al. [41] described four main challenges: immaturity of technology without established standards, usability and user experience, transparency versus unlinkability, and trust management. Both approaches discuss challenges based on the literature and partly on practical experience, not taking a variety of projects into account.

3.3. Solving SSI Challenges

Different approaches try to solve the stated challenges. The SSI eIDAS Bridge [42], which is currently developed within the H2020 NGI ESSIF Lab project [43], makes eIDAS available as a trust framework for the SSI ecosystem. However, it is limited to eIDAS applications. Kubach et al. [44] proposed a trust management infrastructure called TRAIN, offering a trust anchor and automation. TRAIN leverages the global Domain Name System (DNS) and is based on the project LIGHTest [45]. It thereby relies on centralized components, contradicting the SSI paradigm to a certain degree. Alber et al. [46] adopted the trust policy language of LIGHTest for SSI, while Martinze Jurado et al. [47] applied eIDAS LoA to credentials. These approaches try to establish trust by centralized means used within FIM and, therefore, are compatible with the current eID ecosystem. Brunner et al. [48] described two options: (1) a Web of Trust or (2) a hybrid approach integrating certificate authorities.

The bootstrapping of SSI is not stated as a challenge, but holds a practical issue. This includes the "import" of already stored user data, but may also be extended to including more services. The Connecting Europe Facility (CEF) SEAL project [49] links credentials and uses proxies to integrate existing IDPs and SPs. These proxies enable the legacy systems to be used with SSI, but at the same time are against the principles of SSI. SSI systems could be enriched with qualified eID data imported from existing sources. Such a derivation process needs to transform the data and maintain the data's trustworthiness. Abraham et al. [50] proposed a privacy-preserving decentralized eID derivation for SSI, where intermediate parties cannot access the users' attributes in plain.

The approach by Stokkink et al. [51] tries to narrow the gap between more academic SSI approaches on the one hand and functional and legal requirements of governments on the other hand. The authors proposed the utilization of IPv8 as a successor to IPv4 and IPv6, which tightly integrates identities, with a decentralized public key infrastructure (PKI) and an anonymizing SSI overlay. The approach has the advantage of privacy, while federated infrastructures might not be usable anymore.

3.4. Need for Lessons Learned

Several challenges are already addressed, while market research gives an overview of current stakeholders and new projects. Besides the handpicked eID and SSI projects, which were evaluated by Kuperberg et al. [31], no paper has reviewed existing and finished projects for lessons learned. These lessons learned could be contrasted with the stated challenges and are thus the topic of our investigation in the following sections.

4. Taxonomy of Challenges

With both Dib and Toumi [40] and Kubach et al. [41] describing different types of challenges, we first need a generic taxonomy. This taxonomy can then be applied to the projects, helping to identify challenges. In order to establish such a taxonomy, we primarily regarded taxonomies for challenges in IT projects.

Al-Ahmad et al. [52] built a taxonomy of IT project failures based on studies and a literature review. The authors also described domain-specific failures. The well-established taxonomy was adapted and enhanced for this article. Whitney and Daniels [53] concluded that the root cause of failure in complex IT projects is the complexity itself. Therefore, this factor is widely recognized and important for rather large eID projects. Chapman and Quang [54] analyzed research projects, emphasizing that complexity and inside view are major challenges. The review was though limited due to the scope. Nevertheless, we hence counted inside view in the group complexity. Herz and Krezdorn [55] evaluated epic project fails. The authors noted that stakeholder management is one important factor. Therefore, it was added to the taxonomy. Stakeholder management includes time to market, user stories, usability, procurement, and many more. Since security and privacy are increasingly important (see the General Data Protection Regulation (GDPR)), they are additionally considered as nonfunctional factors.

The taxonomy used for this article is shown in Figure 2. It consists of groups containing several subfactors, which can be extended. We highlight those factors we found in the following projects and solutions. For the discussion, we again apply the taxonomy, as the challenges can at the same time be success factors:

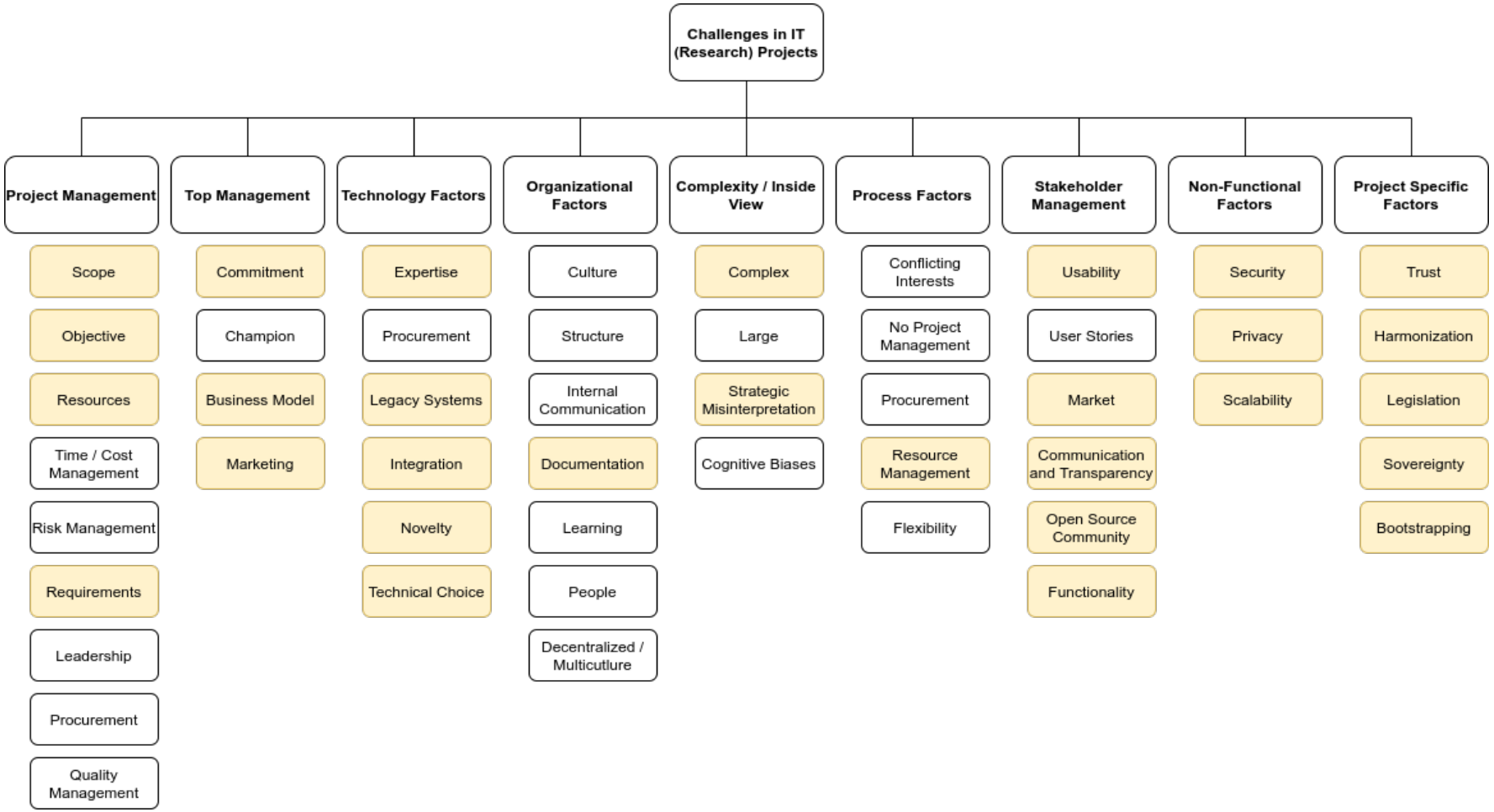

Figure 2. Taxonomy of challenges in eID and SSI projects.

Project management: challenges about the project management itself, including resources (e.g., sufficient and appropriate staff);

Top management: challenges involving the top management. If the top management does not commit to a project, it is likely to fail. Other challenges are related to decisions of the top management, e.g., the choice of business model;

Technology factors: challenges focusing on technological factors, which are not group- or sector-specific. Within research projects, the novelty within technology factors is especially important as it inherently contains uncertainty;

Organizational factors: challenges within the organization, such as culture and learning;

Complexity and inside view: challenges due to complexity and inside view. Large and complex projects are more likely to fail as it is difficult to obtain an overview. At the same time, technology may further advance;

Process factors: challenges due to processes, e.g., flexibility or conflicting interests;

Stakeholder management: challenges centering on stakeholders, i.e., users and other involved organizations. This could lead to misunderstanding the user requirements, failure to gain user commitment, lack of adequate user involvement, and failure to manage user expectations;

Nonfunctional factors: challenges that are closely related to technical factors, such as security and privacy;

Project resp. domain-specific factors: challenges that are specific for the project or the domain. We decided to add legislation, regulations, and sovereignty to the project-specific factors since these challenges are rather specific for eIDs and SSI. Nevertheless, they are present to a certain extent in every project. Therefore, it is possible to introduce another category containing them.

Regarding the challenges Dib and Toumi [40] found, the technical limitations were included in the technological factors. Nontechnical issues were spread across other factors. For example, legacy systems and standards would fall into technological factors, while regulations are project-dependent. Adoption and accessibility belong to stakeholder management. Behaviors of actors can either be organizational factors, if internal, or stakeholder management as well. The four challenges stated by Kubach et al. [41] were categorized as technology factors (immaturity of technology; though also project-specific), stakeholder management (usability and user experience), and project-specific factors (trust management, transparency versus unlinkability). This shows that project-, respectively sector-specific factors are mainly technical factors.

5. Traditional eID Federations

In this section, we provide an overview of selected eID solutions and projects, as well as discuss the results based on the taxonomy.

5.1. Survey of National eID Solutions and Projects

We only regarded eID solutions and projects with traditional FIM. These can be national eIDs, as well as industry initiatives. We did not consider solutions for similar, but highly specific, areas, such as tax or healthcare. However, if the solution provides access to both, it is mentioned. SSI-based projects are reviewed in Section 6.

For each country or project, we indicate the technology involved, the issuer, as well as the type of eID, e.g., mobile. If the history of eIDs or generic e-government provides insights, which other projects may profit from, we add them. The driver behind the eID and its scheme, i.e., public or private sector, is mentioned, if we find relevant information. In addition, we note if the eID is limited to public services or if private services are included. We also chose projects based on the learning outcome for future projects; see the taxonomy. Last but not least, we excluded countries and projects where we could hardly find available

information in English. Thereby, the selected countries are biased towards Europe since eIDAS is well documented, as shown in Figure 3.

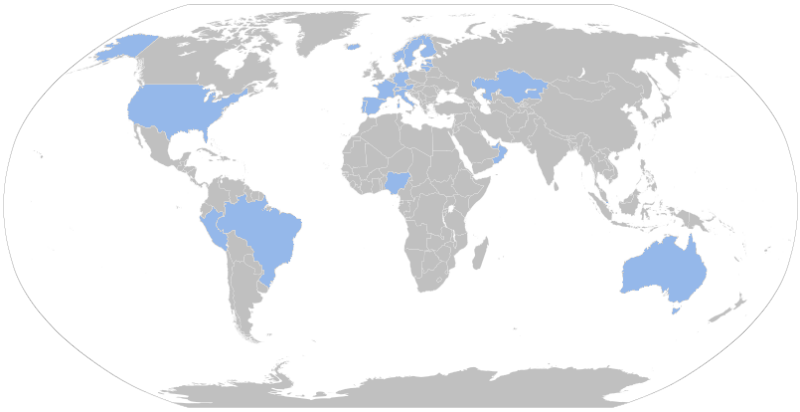

Figure 3. Overview of the selected countries for the eID survey.

5.1.1. Scandinavia

In Sweden, Norway, and Finland, commercial BankIDs are widely accepted.

Norway: In order to use digital services from Norwegian [56] public agencies, several electronic IDs can be applied: MinID, BankID, BankID on mobile, Buypass, and Commfides. MinID is an eID for access to public services with a medium level of assurance (LoA), issued by the National Digitalisation Agency. BankID and BankID on mobile are issued by banks. Buypass can be used with either a smart card or on mobile and gives access to services with the highest LoA. Commfides also suits the highest LoA and is provided by a secure USB stick. Buypass and Commfides are commercial companies. ID-porten is a login portal to public services, which also allows login via an ID-porten account. Interestingly, BankID and ID-porten—and probably the other eIDs—support OpenID Connect, as well as SAML [57,58]. BankID is the most popular eID [59].

Sweden: In Sweden [60], besides the Swedish BankID, two further eIDs exist: AB Svenska Pass and Freja. Freja eID Plus, provided by Freja eID Group AB, is a mobile app, which also can manage and store COVID-19 certificates inside the app. Svenska Pass is issued on the Tax Agency's ID card for the highest LoA. All three are governmental approved for the eID scheme Svensk e-legitimation. Telia ID, issued by the Telia Company AB, is no longer available after an agreement with Freja, but still might be in use. Both countries have distinct federations for different sectors.

Finland: Finland [61] introduced the world's very first eID in 1999 with its smart-card-based solution. As an alternative, TUPAS, a bank ID, requires two of the three methods password, chip card, or fingerprint or similar. Commonly, the combination of password and one-time password (OTP) is used. As the latest addition, a mobile ID with a secure PKI-based authentication and digital signing solution was introduced. Today, e-government relies on the mobile ID, bank ID, or eID card for strong authentication.

Iceland: IceKey [62] is issued by Digital Iceland. Besides public services, private SPs are allowed to use the login service. IceKey comes with a default password, consisting of three words from the Icelandic dictionary separated by dots. The user needs to change the password at first time use. IceKey with a text message (SMS) sent to the mobile phone can be used for multifactor authentication.

Conclusion: These examples show that if governments are not fast enough, then banks and other private companies offer a solution first. This may come with an advantage for the citizen, but does not have to. In addition, a shift to mobile and OIDC (at least partly) can be seen. Last but not least, strong authentication is apparently widely regarded as important.

5.1.2. Baltic States

The Baltic States are comparably young countries. When setting up their governments, they heavily relied on electronic services. However, the progress and extent of online services differ among them.

Estonia: Regarding eIDs, Estonia is arguably the most advanced and fastest country. This came with the downside of large DDoS attacks in 2007 and 2008 [63], resulting in the subsequent use of *blockchain* for all registries called keyless signature infrastructure (KSI) [64]. Estonia [65] utilizes *X-Road* to connect different services and servers. Thereby, users can decide which information is being shared among which institutions. Estonia has officially notified six different eID schemes [66]. Besides the Estonian ID-card, which is a smart card, Mobiil-ID for the SIM card was registered. Mobiil-ID is only issued to owners of the Estonian ID-card. The authentication process is based on Secure Sockets Layer (SSL)/Transport Layer Security (TLS) client certificates, allowing both private and public sector entities to integrate it. In addition, SAML is used between the eIDAS connector and the authentication service, while OIDC comes into play between authentication service and e-services.

Latvia: Latvia [67] offers two cards, an eID card and eParaksts. eParaksts is an e-signature card, which is utilized for mobile eID. If a hardware keystore is used, it obtains a *high* LoA; with software keystore, it achieves only a *substantial* LoA.

Lithuania: Lithuania [68] operates the public-sector-issued contactless identity card Asmens Tapatybes Kortele (ATK), which can also be applied for qualified electronic signatures. For identification for public services, the unique and persistent national personal code is utilized. In addition, a mobile ID is available.

Conclusion: Having none or at least almost no legacy systems led to advanced e-government and pioneering in blockchain. In Estonia, a long-term project targeting multiple changes in government resulted in e-Estonia. Transparency helps citizens to understand the evolution, which is essential when something goes wrong. Estonia provides guidance with its Academy [69], already accepted by several countries including the EaP countries Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine, as well as, Mongolia, Tonga, and Namibia. These examples may provide lessons learned when introducing blockchain in the future. In addition, the mobile ID with different LoAs reaches more users resulting in a rise of eID usage.

5.1.3. D-A-CH Region

All three countries within the D-A-CH region, Germany, Austria, and Switzerland, originally relied heavily on smart-card-based eIDs. This has changed to some extent.

Switzerland: Initially, Switzerland [70] had a smart-card-based eID with the highest LoA. However, the eID ecosystem went through a major revision as it was too expensive and slow, while not reaching the market. With the new eID concept, Switzerland wanted to open the market for private companies to become IDPs issuing recognized eIDs. As an example, SwissID and trustID were chosen: The SwissSign Consortium of SwissID consists of several government-related organizations, insurance companies, and banks, while trustID is provided by CloudTrust, a subsidiary of the ELCA Group. Currently, the status is on hold, as the law was rejected in a referendum.

Austria: The Austrian eID [71] went through a major revision, since the originally issued smart card eID had low take-up. The new ID Austria is a mobile eID open for both the public and private sector. Integration for browser-based services is performed via SAML and OIDC. It also allows app-to-app communication. ID Austria is currently in a pilot operation, integrating passports into the app by the end of 2021.

Germany: The German eID [72] was the first officially declared eID scheme for eIDAS [66]. It is based on the German national identity card and electronic residence permit. Due to the use of Extended Access Control (EAC) Version 2 described in the BSI documents TR-03110, each SP requires an authorization certificate and either an own eID server or a corresponding eID service. In order to obtain such an authorization certificate, SPs usually

need to apply first, including a substantial service fee. Public bodies are excluded from this rule, since every municipality is required to provide its services online by law. To make things more complicated, every federal state can have its own digital identity system, leading to the rather complex, mostly SAML-based federation FINK in Germany. The project OPTIMOS 2.0 [73] provides the ecosystem for the mobile eID, while the project digital identities [74] tries to optimize the app. The mobile app AusweisApp2 [75] can be used as long as the smartphone is equipped with near-field communication (NFC) capabilities and runs on either iOS or Android. The new mobile eID app will currently (October 2021) only work on the Samsung Galaxy S20 series, as so far, this is the sole device that fulfills the secure chip requirements for the mobile eID.

Conclusion: All three countries first relied on smart card eIDs with a high LoA. While Switzerland and Austria were or are changing to mobile eIDs with the hope to increase the usage, the German mobile eID requires high security requirements, which are only met by too few consumer devices and, therefore, users. All three examples show that it is important to have the users in mind when designing eID solutions. The eID solution has to be convenient and beneficial, i.e., provide enough services so that the user has advantages from using it. Hence, a balance between usability and security is suggested.

5.1.4. Southwest Europe

While SAML was predominant in this region, OIDC is gaining a bigger share.

Belgium: Belgium was among the first countries to introduce an eID, which was initially based on the ID card and then evolved into a federal authentication service using SAML. Besides the public-sector eCard [76], a private-sector-driven mobile solution called itsme [77] is supported. itsme is integrated with the public services via the federal authentication service, but also enables private services with OIDC. It is a pure mobile solution bound to smartphones and SIM cards using secure elements. The app is available for iOS, Android, and Huawei. The eID scheme was founded by a consortium of four Belgian banks and three mobile operators, supporting itsme, the eCard, as well as the Foreigner eCard. Belgium has a central portal (belgium.be, accessed on 11 November 2021) for over 800 services. The Flemish ID system supports both SAML and OIDC, running software from ForgeRock [78].

France: Similarly, France [79] uses a central portal (service-public.fr, accessed on 11 November 2021) to access over 900 services. The single-sign-on (SSO) solution is called FranceConnect and utilizes OpenID Connect. The documentation, as well as several repositories are online [80]. The FranceConnect button allows users to connect from existing audited accounts, e.g., from LaPoste or Mobile Connect, to these services.

Italy: Italy [81] has officially declared two eID schemes, Carta d'Identità Elettronica (CIE) and Sistema Pubblico di Identità Digitale (SPID) [66]. Both are public-sector issued. CIE [82] is a contactless smart card as the national identity card following the European Citizen Card specification. The IDP is operated by the Ministry of the Interior, allowing the Italian public sector to use the attributes via SAML. SPID [83] is a federation, joined by several IDPs, but no banks. Authentication is possible with a username and password, along with several variants of OTPs, smart cards, or hardware security modules (HSMs), leading to varying LoAs. Users are allowed to have several IDs, and *none* of them has to be government issued. Due to the pandemic and a bonus for 18-year-old Italians and teachers, the usage of eID has grown sustainably [4,5]. In addition, a shift from SAML to OIDC can be observed.

Portugal: Portugal [84] combines several cards and functionalities into one: Besides the ID, the card can be used for elections, health insurance, social security, as well as taxes. Although the card provides a combined functionality, the databases are decentralized by law. In addition, citizen can make use of the app ID.GOV.PT to store and consult documents, have access to the citizen card, driver's license, or other cards through the smartphone by utilizing the Digital Mobile Key—Chave Móvel Digital—for this.

Conclusion: A central portal, as in Belgium and France, can provide access to several services in a user-friendly way. OIDC may increase the adoption by service providers, as many already run OIDC or OAuth 2.0 entities anyway. APIs and web services can promote the

interoperability between IT systems. At the same time, they make the solution accessible by other sectors. In addition, the *reasons* to use eIDs, such as the pandemic or a bonus, may increase the number of users. By publishing the code and documentation, service providers know the technical details upfront. This could even lead to an active open-source community.

5.1.5. Arabian Peninsula

Different starting points of eIDs within the Arabian Peninsula lead to different solutions. While Oman was an early adopter of the mobile ID, the United Arab Emirates (UAE) started later.

United Arab Emirates: In 2017, it was announced that within the Smart Dubai initiative [85], a unified digital identity based on blockchain technology was going to be developed. The project aims to integrate UAE's SmartPass, a verified identity service with the eID-enabled Dubai ID online service, to form one single system. The UAE [86] eID system conforms to several standards, including X.509 for PKI and ISO/IEC 17799 for the code of practice for information security management. In addition, an app for Android and iOS was released. More and more services became available online during the pandemic [87]. In 2020, the blockchain platform was launched. However, no further information of its use for identities is available. Al Marri et al. [88] outlined the application and potential of artificial intelligence (AI) for Dubai's e-services.

Oman: The Sultanate of Oman introduced a smart-card-based eID based on the national PKI, providing both authentication and signature certificates. In addition, a mobile ID was launched. The mobile ID is driven by the public sector and requires specific SIM cards provided by licensed and accredited mobile network operators. Tam [89] is a government-funded system *free of charge* for citizens, respectively residents, as well as relying parties.

Conclusion: Combining several services and cards is convenient for citizens. A government-funded system reduces entry costs and provides more services. Developing a mobile ID later on, with newer technical standards in mind, leads to different solutions (e.g., mobile apps in comparison to websites and SIM-card-based solutions). More publicly available information and documentation would help others to progress.

5.1.6. Nigeria

Nigeria: Identity is based on a unique national identity number (NIN) used as the identifier in the databases. Enrollment consists of the recording of the demographic data, ten fingerprints, a head-to-shoulder facial picture, and a digital signature. NIN slip, improved NIN slip with a QR code, the national eID card, and the mobile ID app provide access to several governmental services. In order to obtain the app, citizens need the NIN, a phone number to receive an OTP, and a good Internet connection. The App Nimc is available for Android and iOS [90]. Costs appear for verification and private organizations.

Conclusion: Several means of identification help citizens without mobile phones. One option, such as mobile apps, can be funded, while another (smart cards) may not. At the same time, identity theft has a great impact if one unique number is used for identification throughout the life of a citizen [91,92]. Proper procedures and security management have to be in place.

5.1.7. Asia

e-government and, hence, eID is diverse in Asia, where countries range in population size and in per capita GDP. We provide two examples, Singapore, a small country with a high GDP, and Kazakhstan, which is vast in comparison and with a per capita GDP that is more than six-times lower than Singapore's, but both are comparably advanced in eID technology.

Kazakhstan: Inspired by the Baltic States and Singapore, Kazakhstan initiated its e-government project in the early 2000s. The portal (www.egov.kz, accessed on 11 November 2021) went live in 2006, which is now the entry point for several services, e.g., related to healthcare, education, and citizenship. The login options range from password and digital ID, QR codes, usage of OTPs, to an eID on a SIM.

Singapore: Singapore's SingPass [93] is a rather evolved portal, where citizens and businesses can log in either with a QR code and app or password. In addition, face verification at kiosks is planned. The login together with the OTP is required for multifactor authentication. The platform is able to utilize OIDC as well. The apps are available for iOS, Android, and Huawei. With them, citizens can include all documents within one app, from finance to family and education to vehicles. The app has also a digital ID, which users can use to verify their ID with either the *watermarked ID* or the *tap the barcode* button. Next, a peer-to-peer check is planned. SingPass is a government-funded model free of charge to citizen, as well as service providers.

Conclusion: Again, one common portal to access several services helps users navigate. Users benefit from having different login options, though this may come at the price of a lower LoA. In the case of services with a higher risk, a step-up authentication, e.g., with an OTP, could be included, providing a higher LoA when needed. Since the SingPass app is available for several operating systems, it reaches more users. The functionality of the digital ID card provides further benefits for the citizens, while the uptake is increased by the government-funded model. Since relying parties have to pay *no fee*, more services are available for citizens (over 340 governmental and 1400 private services). With ever-increasing services, the security of the app and smartphone comes into focus.

5.1.8. Australia

Australia: Australia was an early adopter of the digitization of government services, already peaking around 1999 [94]. Some states continued, for example, New South Wales and Victoria provided single online platforms. Two critical missing pieces, identified by [95], were a digital ID ecosystem and digital signatures. A national identification scheme was proposed in the 1980s, but was defeated due to privacy concerns [96]. Another attempt in 2006 failed as well. With the Trusted Digital Identity Framework (TDIF) [97], an infrastructure that should underpin the eID Govpass was established in 2019. At the same time, another eID was launched by the Australia Post: Digital iD [98]. Today, organizations and government agencies can apply for TDIF accreditation, having four accredited providers including Australia Post. Both SAML and OIDC are recognized.

Conclusion: This transition also shows that secure data exchange between different government IT systems, internal processes, as well as exchange between stakeholders is essential.

5.1.9. United States

In the U.S. [99], there is *no* federal law to require citizens to obtain an identity card or any other identity credential. However, in order to, e.g., open a bank account, obtain a job, or pay taxes, some kind of government-issued identity document is needed. While there exists no national ID, there actually are government-backed identity systems—provided by different federal, state, and local entities. This legacy infrastructure is around 20 to 30 years old and was not designed for today's online world. Instead, the Social Security Number (SSN) is often used instead of an eID. As a result, the industry has filled this gap. Attackers though have also caught up, e.g., with identity theft [100].

Driver's license: Besides the SSN, the driver's license is an important document that almost every adult citizen has. Some state initiatives tried to evolve it. For example, a mobile application in Colorado, Idaho, Maryland, and Washington, D.C., to digitally access the driver's license was one of the awarded six pilot projects in 2016 [101]. Similarly, Arizona launched an app called Arizona Mobile ID [102] for Android and iOS to allow access to vehicle or driver's license information and services related to it. These projects have a limited scope and cannot be seen as traditional eIDs, but may provide access to e-government services.

Wyoming: In June 2021, the digital identity legislation was enacted. According to the bill, the natural person has autonomy over her or his personal digital identity [103]. Already since 2020, another bill enabled residents to display their IDs on smartphones as

a supplemental option to physical IDs. Other states have proposed or operate digital ID programs, although several questions concerning security and privacy came up.

Conclusion: In order to keep up, the development of a next-generation identity system would need to be prioritized including a change of SSN usage and educating online users. Funding is required to change the infrastructure. At the same time, a focus on privacy could reduce the amount of breached data. As most citizen have a smartphone, this should be the preferred device. Since technology is not all, laws, regulations, and policies need to be adapted at the same time. If more states enroll in an eID system, a trust framework with a scheme such as eIDAS instead of a federal eID could be established.

5.1.10. Latin America

Some Latin American countries, such as Peru, have a running eID system, while others struggle. All countries except Mexico and Brazil offer a birth registration system, which is the basis for issuing an ID. However, Women in Identity [104] estimates that three million children under the age of five are living without formal identification documents. With the COVID-19 pandemic, the numbers are presumably increasing. In addition, marginalized sections of the population are not officially registered including indigenous population, people of Africa-American origin, those with a migration background and their children, and poor people [105].

Peru: The Peruvian digital DNI Electrónico (DNIe), promoted since 2013, was considered the best identity document in Latin America in 2015 [106]. Quiroz et al. [36] gathered requirements for a new eID while focusing on eIDAS and European eIDs.

Brazil: Brazilian citizens are issued several different documents since each state has its own model. Similar to the U.S., the Cadastro de Pessoas Físicas (CPF) (Natural Persons Register) is essential to open bank accounts or rent a car. While the CPF is used as an identification number, the CPF document neither provides a photo ID nor other elements to prove a person's identity. The resulting problems included 45.4% of global cases of credit card fraud in 2020 [107] and the largest leak of citizen's personal data in 2021 [108]. As the databases are not unified, cross-checks to confirm that the person who is, for example, trying to open an account is the person who they claim to be are slow. The only unified system is the Carteira Nacional de Habilitação (CNH) (National Driver's License), which is not mandatory. The urge for digital identification is increased by the high number of Internet users.

Conclusion: A birth registration system is the basis for proper identification. Registering babies right at hospitals and by doctors could be a first step towards reducing the number of unregistered children. Orientation on the best practices and successful projects will help to mature this. With the migrant crisis [109], the number of persons without an ID and the missing interoperability between the birth and host countries' systems are challenges to overcome. Interoperability might be gained by adopting the concept behind eIDAS or eIDAS itself. The Dominican Republic has prevented Haitian-descended people born in the country from gaining an ID, resulting in a counter-campaign [105]. This shows that national IDs and eIDs can be used to exclude groups of citizens.

5.2. Lessons Learned from National eIDs

Above, an overview of several national eIDs—systems, as well as projects—was provided, from which we comparatively summarized and extracted the essential aspects.

5.2.1. Summary of eIDs

All in all, a certain shift from SAML to OIDC can be seen, supporting authentication with the eID for private companies via an API and mobile apps. Several countries provide multifactor authentication with OTPs for stepping up the current authentication to a higher level of assurance. Therefore, the entry level to use the mobile ID is lowered. A detailed summary of the evaluated eID solutions can be found in Table 1.

Table 1. Summary of national eIDs.

Region	Features	Lessons Learned
Scandinavia	Dominant: bank and mobile ID Protocols: SAML and OIDC, LoA: medium to high	Solution according to business needs; usability and functionality attracts users
Baltic States	Dominant: mobile ID Protocols: SAML and OIDC Technology: connector, blockchain for registries LoA: different	Starting from scratch can be fast; security is essential and might lead to blockchains; different LoA levels depending on the smartphone hardware ease the usage
D-A-CH Region	Dominant: (formally) smart card Protocol: SAML Technology: eID ecosystem, LoA: high standards	Revision with a shift from smart card to mobile; usage of smart cards is low; opening up to the private sector helps speed up; take user needs into account
Southwest Europe	Dominant: mobile ID with apps for different OSs Protocols: SAML and OIDC Feature: one portal	Portal as single point of entry; OIDC easier for apps; different LoAs dependent on the authentication method; features of the solution equal benefits for users; APIs for interoperability; documentation for developers
Arabian Peninsula	Dominant: unified app for iOS and Android Technology: maybe blockchain usage	Increasing number of services helps to reduce contacts; funded system for more services; open source and information would help others
Nigeria	Dominant: mobile ID	Funded models for one type; different forms of identification
Asia	Dominant: mobile ID apps for different OS Protocols: SAML and OIDC Authentication: different methods	Different authentication methods help users; single portal as entry point; public and private services provide a benefit for the user; free of charge helps uptake
Australia	Protocols: SAML and OIDC Technology: several IDPs	Secure data exchange among government IT systems is important; establish processes; exchange between stakeholders; IT is always progressing; resources and strategies are required to keep up
United States	Protocols: no federal system Legislation: no law for this Technology: partly private companies instead; different alternative identifiers	Legacy systems can lead to more identity theft and other incidents; education of users is important; funding for modernization; privacy is essential; adaption of laws
Latin America	Biometrics: mostly Otherwise: diverse	Learn from the best; birth registration system as a basis; harmonization and interoperability among countries; excluding groups of citizens possible

5.2.2. Lessons Learned

In the following, we want to highlight the challenges we found in the projects based on the taxonomy described in Section 4. An overview of the found challenges is shown in Figure 4.

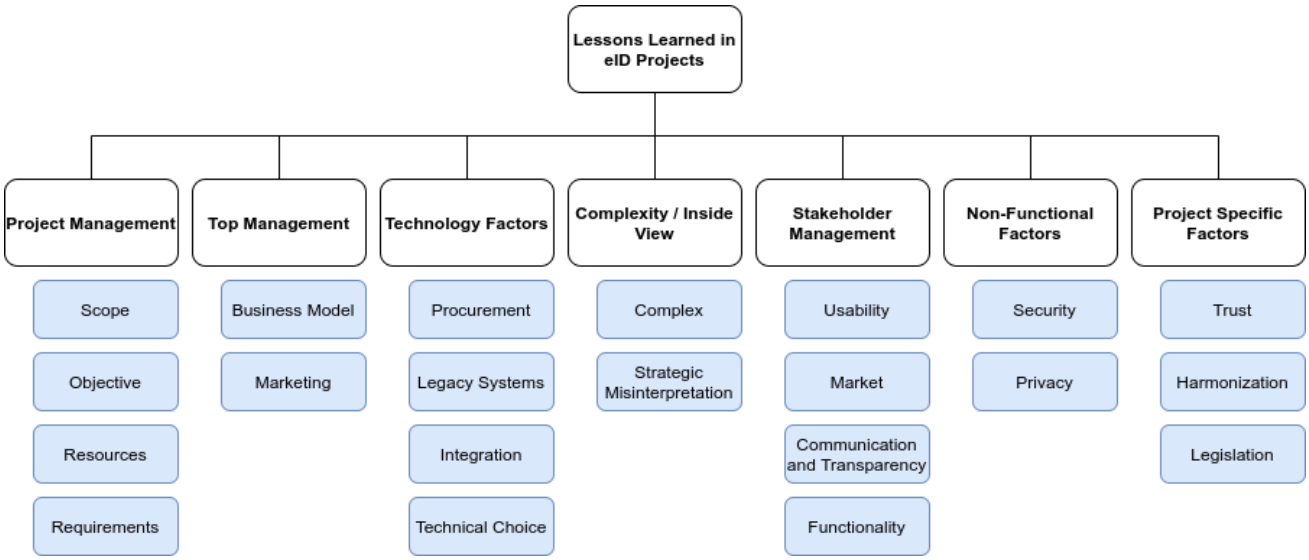

Figure 4. Taxonomy based on challenges in eID projects.

Project and top management: With respect to legacy systems in Australia and the United States, we noticed that the IT and, thereby, identity management are always changing and that resources are needed. Singapore in comparison to Germany has a government-funded model that is free of charge, which increases the amount of services provided to the citizen. Other systems, such as birth registration, are the foundation for identification, whereas the orientation on best practices and good examples help it to mature.

Technical factors: While eIDAS in Europe is based on SAML, different countries enable OIDC in addition. OAuth 2.0 and OIDC are used by a majority of web services, helping them to integrate eIDs. This transition also shows that the architecture should be as technically neutral and modular as possible, so that different layers can be exchanged. Private organizations' services can more easily be integrated if documentation and APIs are publicly available. This goes hand in hand with the protocol OIDC.

Complexity and inside view: We noticed that the complexity of the project while not taking technological changes into account may lead to a solution with a small user base. Furthermore, just focusing on one's own project may result in several solutions in parallel; see Australia. As the field is evolving, it is not only one project to establish a solution, but several projects are required to keep up.

Stakeholder management: It is important that the projects take the user into account, as a solution without users is a dead end. This can be seen, for example, with the limited smart card usage in the D-A-CH region. The eID and digital signature are issued by the same process, which may provide more benefits for the users. If the user has advantages from using an app, the solution attracts more users in turn. A single portal as the entry point to access different services helps users find the services they need. If more services participate, including private services, the users have more value. This can be seen, e.g., in Italy and the UAE during the pandemic. Looking at different public GitHub repositories, open-source strategies, online documentation, and Estonia's e-Government Academy, publicly available information, transparency, as well as exchange are helpful to (1) gain the acceptance of the citizens and (2) enable other entities and states to participate and progress. Internal and external stakeholders, as in Australia's case, need to communicate with each other. ID systems can be used to exclude groups of citizens, while others, e.g.,

migrants, have lost or destroyed their identification document with consequences for their future steps [110].

Nonfunctional factors: Besides Estonia, also Australia suffered from a large DDoS attack in the last few decades [111]. One of the consequences in Estonia was KSI, the blockchain backing up the registries. Looking at the U.S. and Brazil, we noticed the danger of identity theft, data leaks, and other identity-related incidents. As a result of an investigation, the international hotel group Marriott was fined GBP 18.4 M after hackers stole the records of 339 million guests [112]. According to the ForgeRock 2021 Breach Report [113], attacks involving usernames and passwords increased by 450% in 2020 from 2019. However, also contactless smart cards can be attacked due to the user's NFC-equipped smartphone [114]. These examples emphasize the importance of security. In addition to securing the system, the users need to be educated. This is especially relevant due to phishing attacks, which target the end user. eID is obligatory for e-government. Otherwise, providing e-services is difficult, as can be seen in the U.S. The use of personal data is strictly regulated by law. By utilizing biometrics, security can be increased, but this is also a target of rising privacy concerns. At the same time, privacy concerns come up when several cards are tied to an eID. With either (1) tell us once [115–117] or (2) decentralized data, the concern may be reduced. Thereby, if citizens could be the owner of their own data, privacy would be improved. For example, in Estonia, citizens can control their data with X-Road. Another privacy-by-design research direction is SSI, which is discussed in Section 6.

Project-specific factors: The core question is how to identify people, businesses, and other entities. This can range from traditional IDs to unique numbers (e.g., SSN) and other identifiers. It however has to be usable for the end user. Adopting LoAs and contracts, the entities within a federation trust each other. Depending on the authentication, the trust in the user is estimated. Secure elements provide a higher level, while passwords present almost no trust. Authentication for a high LoA may lead to few users. A compromise between usability and security is step-up authentication, where the additional factor is provided only when required. In the long run, harmonizing schemes such as eIDAS, when established as world-wide standards or through technical adapters, as shown with the translation of attributes in SAML [118], may reduce costs and simplify adoption. Other countries, e.g., Azerbaijan, already recognize and utilize eIDAS. Regarding the U.S., we noticed that legislation has to adapt to the changes as well. With the eIDAS regulation in the EU, the 27 participating member states had to adopt it, in order to make eIDs interoperable. Interoperability is needed, e.g., to master the migration crisis in Latin America.

6. New Directions with Self-Sovereign Identity

In this section, we provide an overview of selected SSI projects and initiatives, as well as the results gained from the evaluation based on the taxonomy.

6.1. Survey of SSI Projects

We only considered eIDs that have or had an SSI project. Our survey focuses on the evaluation of the intersection between government-issued eIDs and SSIs. Our analysis of related work for this intersection showed that there is no systematic and current evaluation of it yet.

For each country or project, we indicate the technology involved. We did not consider general blockchain-backed e-government activities such as e-voting, taxes, healthcare, or similar unless these activities create an independent eID. Furthermore, we did not regard blockchain-based IDs in a closed ecosystem without government actors. We also selected projects based on the learning outcome for future projects. Therefore, we indicate the lessons learned. Last but not least, we excluded countries and projects where we could hardly find available information in English. The selected countries are shown in Figure 5. As Europe has several initiatives, it is highlighted in lighter green.

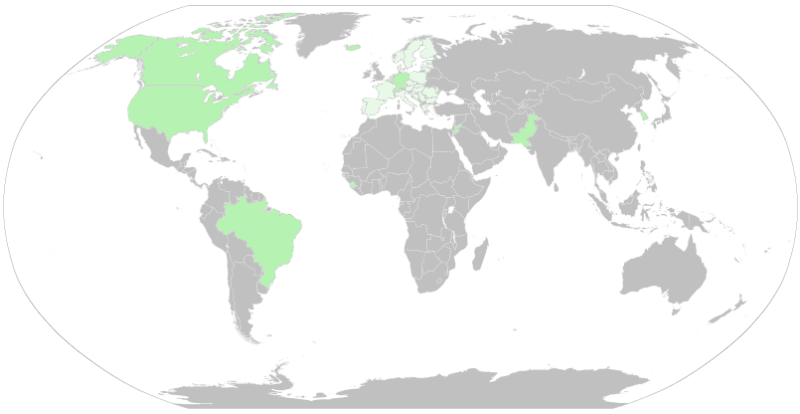

Figure 5. Overview of the selected countries for the SSI survey.

6.1.1. Europe

The European Commission plans a revision of eIDAS [119], which as of today includes a digital wallet. This already shows the direction in which Europe is proceeding. Several EU projects, ranging from KRAKEN [120], SEAL [49], and mGov4EU [121] over eSSIf-lab to Gaia-X and CONCORDIA [122] target SSI in different proportions. In addition, the European Blockchain Services Infrastructure (EBSI) [123] aims to become a gold standard digital infrastructure to support the launch and operation of EU-wide cross-border public services leveraged by blockchain technology. The EU Self-Sovereign Identity Framework (ESSIF) [43] intends to implement a generic SSI capability.

Germany: In Germany, the showcase program Secure Digital Identities [32] turns out to work as a magnet, with more and more organizations joining one of the selected projects. This could even have effects on the neighboring countries. Especially IDunion [124] and ONCE [125] have obtained momentum when comparing the initial and current list of partners. IDunion was originally focusing on the German states of North-Rhine Westphalia and Berlin, using Hyperledger Aries and connectors for OIDC, the Lightweight Directory Access Protocol (LDAP), and SAML. ONCE initially concentrated on the state of Hesse, as well as cities and districts in Bavaria and North-Rhine Westphalia. The three use cases comprise regional e-government, mobility, and hotel and tourism, while building on OPTIMOS 2.0, in addition to traditional SSI. Last but not least, several private initiatives and projects are active, including FIDES [126] and lissi [127].

The Netherlands: The Netherlands are also active in SSI. In 2018, Trustchain started to evolve [128–130]. In the latest publication by Stokkink et al. [51], described in Section 3, they tried to narrow down the gap between scientific SSI and government. The approach has the advantage of privacy, while the federated infrastructure might not be usable anymore.

Unsuccessful projects: However, not all past projects went into production. ZugID in Switzerland [31] was a digital, blockchain-based ID using uPort. The project has been terminated, but future reuse of the results might be possible. At the end, 267 citizens had a digital ID. One reason for the small number might be the limited number of services. In the finale state, elections and bike renting were the only *two* available services, as developing them requires resources. The Flemish government has *withdrawn* from the project Blockchain on the Move [131]. As a result, the remaining initiators have decided not to progress further with a third phase of the project. No additional information about the projects is available. What seems to be important, though, are sufficient *resources* (especially human, hardware, financial).

Private projects: The DIZME Foundation consists of several private organizations and startups. DIZME [132] provides eIDAS conforming to SSI with all LoAs based on Sovrin. Users with self-declared information obtain LoA 0, while LoA 1 is provided with automatic checks. Trusted identifiers elevate the user to LoA 2. DIZME leverages its Trust Over IP metamodel [133] and creates a governance framework. Several other projects are starting [29].

Conclusion: Several public, as well as private initiatives try to enable SSI for citizens. At the same time, the eIDAS regulation is adopted. The member countries have to make the next move in the near future. While especially IDunion and ONCE have the potential to gain attention in Germany, as well as in neighboring countries, the shear number of initiatives and projects makes it hard to make an overview. Although competition can help, the projects should profit from each other by establishing an ecosystem, in order to boost the development. This is especially important as resources are needed to progress successfully. Regarding Trustchain, the question arises how the transition is managed and what parts of the legacy infrastructure can be reused.

6.1.2. Sierra Leone

Sierra Leone: Sierra Leone is not a classical eID SSI use case in the sense of the article, but shows ways around the lack of formal identification. Sierra Leone is addressing the challenge to provide identities to the unbanked and formerly unbankable with the Kiva Protocol [134], based on Hyperledger Indy, Aries, and Ursa, leveraging SSI. Around 80% of the citizens of Sierra Leone are unbanked. Two of the major barriers to accessing financial services are a lack of (1) formal identification and (2) a verifiable credit history. The Kiva protocol issues digital identification to all citizens eligible for a government-issued ID. Formal and informal financial institutions, from banks to shopkeepers giving credit, can help to contribute to the credit history of a person. In a first phase, identities were digitized, and then, these digital identities were used to create nonduplicated, nonreusable, and universally recognized national identification numbers. A challenge is the *missing Internet access*, though. Kiva is based on DIDs, using Hyperledger Indy as the underlying blockchain layer. Biometrics is seen as yet another attribute. Thereby, biometric data does not serve as the identifier, but the verification.

Conclusion: The use case of Kiva in Sierra Leone shows that even in a country with many citizens neither having a formal identification nor a verifiable credit history, SSI projects may help the citizens participate. At the same time, no Internet access may lead to problems. A similar situation may occur for citizen with no smartphone at all, dying batteries, forgotten or failing phones, or areas with no connectivity.

6.1.3. Refugees

Different projects: Similar to Kiva in Sierra Leone, the World Food Programme's blockchain-based Cash-Based Interventions provides some kind of identification and payment system for Pakistan's Umerkot village and 10,000 Syrian refugees in Jordan [135], running on a variant of the Ethereum blockchain. Another example is the Rohingya Project [136,137]. Other fringe groups, profiting from SSI projects, are poor farmers in South America and HIV patients in Africa [138].

Conclusion: In the exemplary projects, SSI provides identities to refugees, which typically (willingly or unwillingly) have no identities and documents. This may be a direction for further groups of persons without documents or a means to obtain the required documents. With more publicly available documentation, these projects may lead toward further SSI projects. Margie Ceesman [139] concluded that SSI is simultaneously the potential enabler of new modes of empowerment, autonomy, and data security of refugees, as well as a means of maintaining and extending bureaucratic and commercial power. Although SSI has great potential, it also comes with risks that we need to tackle.

6.1.4. South Korea

Similar to Singapore with SingPass, South Korea has had an increased use of digital and mobile eID apps. In comparison to Singapore, the provisioning of mobile ID services is privatized. This change was caused by criticism as users were required to use multiple software programs. So far, only the driver's license is digitized. Nevertheless, the increase in privatization is also a concern.

Busan: Busan, the second-largest city in South Korea, has been the nation's regulation-free blockchain zone since 2019. Coinplug, the official operator, launched the SSI app called B PASS [140] for Android. Based on DIDs, B PASS is a single platform offering authentication for several public and private services including the Busan Citizen Card, Mobile Family Love Card, Library Membership Card, Digital Voucher, and B tour. One example is the public safety report, where citizens are encouraged to anonymously report disaster situations by a reward system. However, in order to roll out the solution to the whole country, changes to the *laws* are required.

Other projects: The project in Busan is not the only one of its kind. For example, the Korea Internet & Security Agency (KISA) implements a blockchain-powered employee ID through a smartphone app. Similarly, Nonghyup Bank (NH Bank) introduced a blockchain-based mobile employee ID. As in some other countries, Korea has a DID Alliance.

Conclusion: Alliances can enable exchange among different projects and initiatives, helping to tackle problems and speed-up the progress. Limited projects provide more controllability. These projects can then be rolled out in the country. Changes to the laws have to go hand in hand with the technological evolution. The more information is available in English, the more easily others can profit from the gained experiences.

6.1.5. British Columbia, Canada

BC: British Columbia launched OrgBook BC [141], a searchable directory of public, verifiable data issued by government authorities about businesses in British Columbia. OrgBook BC is an exemplary service of the Verifiable Organizations Network (VON) using Sovrin. The development was helped by another parallel effort in British Columbia called BC Dev Exchange [142]. After adding BC government services to the VON ecosystem, the OrgBook is going to be deployed in other jurisdictions. So far, Ontario has its own VON architecture. Then, interoperability across all communities is the primary goal. This progress goes hand in hand with the *tell us once* policy, pioneered by Estonia and being most mature in the Netherlands according to Naeha Rashid [115]. This policy means that if you provided your data to one government agency, you will never be asked for it again from another.

Conclusion: The method of BC [143] can be reused by other projects: think about the problem while keeping the users in mind, find like-minded groups to boost development, choose the most suitable open-source framework, and contribute your code again to the open-source community, such as on GitHub [144].

6.1.6. United States

In the U.S., different states started SSI projects with slightly different focuses. Two examples with enough documentation are explained, as follows.

Homeless people: More than 500,000 people experience homelessness in America every day [145]. The California Blockchain Working Group [146] states two challenges they want to tackle with SSI: (1) faked driver licenses and (2) homeless people without documents at all. Without an ID, homeless people are often trapped in vicious cycles as they are excluded from public services, such as healthcare or funding. Therefore, Austin, Texas [147,148], and The Bronx, New York [149], tried to solve this issue with blockchain identity solutions as these records cannot be destroyed. After a test pilot targeting the homeless population in Austin, MyPass Austin running on a permissioned Ethereum-based network was offered to all residents. One preliminary result was the privacy concern when requiring biometrics. The source code is online on GitHub [150]. New York City and the organization Blockchain for Change trialed a similar project. In 2017, the organization handed out Android smartphones to 3000 homeless people already loaded with the app Fummi. Both projects seem to be inactive though.

Illinois: In Illinois, several documents, ranging from task force final reports over legislative blockchain and distributed ledger task force meeting agendas to procurement bulletins exist. However, no actual projects were found on the Illinois Blockchain Initiative page [151].

Conclusion: Both directions are important, practical projects and legislative changes. SSI could be a means to provide identification and governmental documents to homeless people, as well as other fringe groups. Nevertheless, resources need to be available.

6.1.7. Latin America

Several projects, but also a Latin American Alliance were started. LACCHain is an alliance for the development of the blockchain ecosystem in Latin America and the Caribbean launched in 2018 [152]. We want to highlight the number of projects in Brazil.

Brazil: The public administration is proactively encouraging SSI projects [153]. Examples include Identity Tech, bCPF, and eID+. Identity Tech was a project in collaboration with Microsoft, building on uPort/ConsenSys as a gateway to services offered by the public administration with DLTs. bCPF was a government-to-government pilot project aiming to simplify the processes to access government services using DLTs. eID+ was a project from the private sector, in which a Swiss company chose Brazil as the headquarters for SSI projects in Latin America. However, no recent information could be found for these three projects.

Conclusion: Alliances may bundle efforts and help to successfully establish SSI solutions. Even though incentives help to start several projects, this does not inherently mean they are successful.

6.2. Conclusions about SSI Projects

An overview of several SSI projects and initiatives was provided—most of which are government based. In other cases, (nonprofit) organizations were or are involved. First, we give a brief summary before extracting the essential aspects and comparing them with eID solutions.

6.2.1. Summary of SSI Projects

While some projects are progressing further and further (e.g., BC, refugees, and Busan), others terminated before reaching the finish line (e.g., ZugID and Blockchain on the Move). In order to use the lessons learned from the projects, information needs to be online. Transparency is not only important for following projects, but also citizens. This may come with a shift of the culture. We tried to collect as much information as possible to draw conclusions. Table 2 shows a summary of the presented SSI projects. We concluded that an open environment for exchange and boost is important. With an open-source project, more people can participate. However, at the same time, it is not a guarantee to success. Resources are equally important. If only a few persons are involved in the projects, the change in participation has a bigger impact. Furthermore, resources in the sense of time, hardware, and money, to name a few, are required. Last but not least, we want to emphasize the technological choice. As SSI is still evolving, the technology might change. Selecting the best-fitting option while building a technology-agnostic or technology-neutral, as well as modular architecture would help adaptation in the case of unforeseen changes.

Table 2. Summary of SSI projects.

Country	Status	Lessons Learned
Europe	Diverse (from starting to stopped)	Participants: public and private bodies Legislation: eIDAS Version 2; national law has to follow Projects: with potential to gain attention, Technology: diverse Community: competition, but common efforts needed as well, Challenge: how to integrate SSI in infrastructure, Lessons learned: resources needed.
Sierra Leone	Productive	Participants: Kiva and public bodies Technology: Kiva protocol on Hyperledger Indy, Goal: empowering citizens, Challenge: partly no Internet access.
Refugees	Up to productive	Technology: Ethereum, partly unknown Goal: empowering refugees with no documents Lessons learned: SSI comes with potentials and risks.
South Korea	Progressing to productive	Participants: public and private bodies Technology: e.g., Metadium Enterprise Platform Legislation: takes time Lessons learned: alliances enable exchange, documentation in English
British Columbia	Progressing	Participants: public and private bodies Technology: Sovrin Lessons learned: (1) analyze problem; (2) peer-groups to boost development; (3) choose most suitable open-source framework; (4) contribute code to open-source community.
United States	Diverse (from started to stopped)	Participants: public and private bodies Legislation: in parallel with technology Goal: resources to empower homeless people, Lessons learned: open source does not automatically mean success.
Latin America	Diverse	Participants: public and private bodies Technology: diverse including uPort Goal: improve administration Lessons learned: alliances bundle efforts; incentives do not necessarily lead to successful projects.

6.2.2. Lessons Learned

In the following, we summarize the conclusions found with the SSI projects based on the taxonomy, as shown in Figure 6.

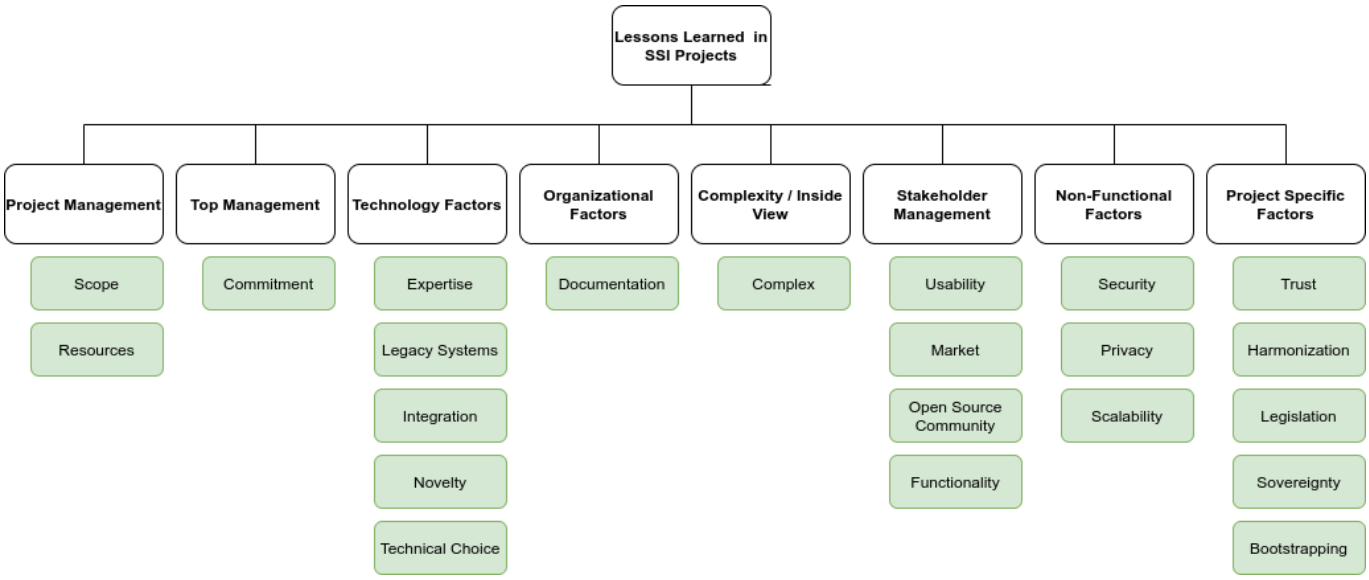

Figure 6. Taxonomy based on challenges in SSI projects.

Project and top management: What we noticed from the ended projects within Europe is that resources are important. ZugID did not continue, as adding services requires manpower. A similar move can be seen with Blockchain on the Move. Stimulation, such as in Brazil, does not necessarily lead to successful projects.

Technical factors: With regard to ZugID and Identity Tech, we observed that uPort is no longer maintained. Especially in the beginning, systems may change more often as SSI is still evolving. Technical neutrality and modularity may help to integrate and adapt SSI. Determined by the type of architecture of eID in parallel with SSI, this might become even more relevant if all services have to change. Since SSI is evolving, we are still using the current (in the future legacy) systems. As not all users will change to SSI at the same time (or at all), the legacy systems may be running for several more years. Dependent on the SSI architecture (see Trustchain in The Netherlands) and bootstrapping, either an integration is somehow possible or everything needs to be built from scratch. In the next section, we discuss possible scenarios. In order to enable the tell us once policy, further changes are required. Integration is as important with SSI as with eID. Another issue may be missing Internet for the end user (no data volume, no Internet connectivity, blackout, etc.); hence, an offline version should be added.

Nonfunctional factors: Security is a primary goal, with methods ranging from security by design to code reviews and software diversity. SSI is per definition centered on the users, which are in full control of their data. Dependent on the integration into the current infrastructure and the architecture, third parties might be involved. These can reduce the privacy [51]. In addition, biometrics for authentication are typically required. Citizen may have concerns about the usage. Even with SSI, the users need to be educated and further research for new phishing methods and countermeasures are mandatory.

Stakeholder management: Actual users and good usability are essential for the success of a project. As an incentive to use the app, the user must have a benefit for doing so. The core question is still the same: How can citizens be identified initially and on-boarded securely? The self-sovereign identity exists primarily on the citizens' devices, requiring robust procedures to handle the loss or theft of devices. While SSI projects in fringe groups are (partly) in production, governmental SSI is still at the beginning. At the same time, as the exchange between all stakeholders and projects in an ecosystem of progress is important, advanced projects should be included even if the target group is limited. IDunion and ONCE, for example, seem to be a good start.

Project-specific factors: With established eID federations, trust between the entities is provided with LoAs and contracts. Similar concepts are needed with SSI. The trust—or lack

of it—in the user has not changed. Harmonizing schemes, such as the standards developed by the Hyperledger Indy and Aries projects, aim to help show opportunities, pave the way for adoption, and reduce costs. Adoptions of those standards, as done with eIDAS, further accelerate and solidify a common ground. What we see with eIDAS in Europe and developments in South Korea is that legislation has yet to adapt. Otherwise, governmental SSI is not possible. If changes in regulations take longer, then the technical progress may come to a hold.

7. Discussion

In Sections 5 and 6, we evaluated current and past eID and SSI projects in order to gain lessons learned for future use. We regarded several projects, but—especially when it comes to eID—could not describe them all. Therefore, we had to choose based on the stated aspects. The selection is biased towards Europe, as more information is available in English and the eID systems are rather prominent in the research. We tried to include projects from all regions. Nevertheless, we may have overlooked a project with lessons learned that is now missing. The most common aspects though should be stated in the evaluation. When it comes to SSI projects, evaluating projects with another scope may bring insights since the technology is new and every lesson learned is important. We point to specifics in this section, when appropriate, though additional research is required. First, we provide general lessons learned and some outlooks based on the taxonomy, before we discuss further findings.

7.1. Challenges Based on the Taxonomy

To start with, we regarded challenges within eID projects and solutions in Section 5, followed by those within SSI projects in Section 6. Taking further information into account, such as interesting projects and approaches, we provided a generic discussion about the challenges, as well as the lessons learned. The structure was based on the taxonomy. Even though the project management and top management discussions were comparatively short, it may be that not all information is available online. The taxonomy was already shown in Figure 2.

7.1.1. Project and Top Management

Project management: Without resources, the inclusion of several services is not possible. Hence, the users do not or only at a lower level benefit from the project. The loss of resources may also lead to the end of a project. Therefore, having enough and adequate resources is important. Providing a like-minded group may soften this issue to a certain extent.

Top management: The eID project in Dubai had support by the top management. Another example is British Columbia. This may also be the case for the EU in the future. Support alone is though not enough; see the projects in Brazil. In contrast, marketing for eIDAS at the beginning could have been improved. Different business models may help or hinder the uptake, as shown in Singapore, respectively Germany.

7.1.2. Technical Factors

Technical choice: In the EU, we noticed a change from SAML to OIDC, although eIDAS is based on SAML. Running both protocols in parallel has the advantage that the integration of (private) service providers is simplified. SPs can make use of an API, while many already have OIDC in place. In addition, OIDC provides greater flexibility for mobile apps. Nevertheless, it adds complexity. In contrast to FIM, SSI is still a new technology, which is rapidly evolving. In some terminated projects, such as ZugID and Identity Tech, the technology is no longer maintained. This may happen again in the future, since SSI is still progressing. Therefore, the best-fitting solution should be chosen. At the same time, technical neutrality and modularity are important, so that changes do not require a complete redevelopment. This is not only essential for the current development of SSI, but

also for future directions and classical eID. Based on the observations in this paper, the most commonly used technologies for building SSI projects are Hyperledger Indy and Aries, as well as implementations of the DID and VC standards using the Ethereum blockchain. Another requirement for the technical choice could be an offline version, so that people without Internet (willingly or unwillingly) can participate.

Novelty: The immaturity of the technology may lead to redesigns and redevelopments, when protocols and technology change. uPort is, for example, going to end. Zero knowledge proofs as one of the key concepts for SSI are still at an early stage. Revocation, recovery, backups, and the right to be forgotten are further research questions. Additional protocols will be designed in the future. When starting with SSI, there is an uncertainty if the technology will stay the same in the next few years and how interoperability among solutions may be gained. Mature and robust decentralized registries are necessary for scalable SSI solutions including transactionality for issuing identifiers and proofs for credentials and solid regulatory frameworks. Regional efforts try to develop local networks, such as EBSI in Europe and LACChain in Latin America and the Caribbean.

Legacy systems and bootstrapping SSI: Legacy systems, as in Australia and the U.S., may put innovation on hold. Often, as in Australia, the U.S., or Scandinavia, other organizations then try to launch their own system. This is not necessarily a bad development. Private companies need to go with the market and can boost the development, as in Scandinavia. At the same time, this comes with risks, for example, regarding privacy. Therefore, some regulations are useful. This will be the same with SSI. In situations where no legacy system was running or the legacy system was too complicated, such as for refugees or homeless people, projects were launched fast. In other countries, such as Brazil, this was not the case and would probably require a birth registration system first. However, changing the whole infrastructure might not be a solution as it requires many resources. Two primary architecture options for 5G deployment from Long-Term Evolution (LTE) exist: non-standalone and standalone. While non-standalone enables both with additional elements, standalone describes LTE and 5G in parallel architectures. Both may be deployed for the progress from eID to SSI as well since not all users may change to SSI at once. Current eID systems store all the identity information, which is required to be imported to SSI. Besides each user importing her or his credentials, other approaches exist as well. Proxies might enable more SPs and IDPs [49]. With SPs, more services are available, and therefore, this provides a higher benefit for the users. By adding proxies on the side of IDPs, the current data can be used further. On the downside, this counteracts the principles of SSI. A privacy-preserving decentralized eID derivation for SSI [50] is another approach that needs to be taken into account. In addition, some services might not even (willingly or unwillingly) enable FIM. The straightforward approach is to help them enable FIM or SSI. Either as an interim solution or if services do not want to cooperate, CanDID [154] based on DECO [155] may be another way. CanDID by Maram et al. empowers the end user by issuing credentials from existing, unmodified web service providers. On the other hand, this may lead to security issues.

Integration: While publicly available documentation and APIs enable the integration of private organizations, publishing information about SSI projects and also transparently showing mistakes, as well as the lessons learned can help the citizens gain trust in the government and, at the same time, provide meaningful input for further projects. Good examples to increase participation are governmental funding models, for example in Singapore, and an innovative environment, as in British Columbia. Especially with the new SSI direction, an innovative environment can help boost the development.

7.1.3. Stakeholder Management

User: Even though the users gave positive feedback for the election via ZugID, the app gained only a few users. The main reason is probably the small amount of services (two) in the end. This example shows two main elements: usability and benefit for the user. The more services a user can use, the more she or he benefits from the app and, thereby,

the eID, respectively SSI solution. As shown in British Columbia, it is essential to enable services to participate. With the change from the eID to SSI, this again gains importance. If the burden is too high, the users will not use the solutions; see the smart card IDs in the D-A-CH region. Biometrics is an easy method to authenticate, though spoofable if applied as a single factor [156]. Step-up authentication, for example with an OTP, is one option to balance security and usability. Both usability and benefit are again important for SSI. If both are not reached, the projects are dead ends. Even with SSI helping fringe groups, such as homeless people, identify themselves, the original problem is not solved. Without access to hardware and the Internet, SSI does not provide identification. This goes hand in hand with the challenge of portability.

Usability, adoption, and acceptance: The user's needs should be at the center of the project. Without users actually consuming the product, it is bound to fail. Transparency during the project allows citizens understand what is going on, what went wrong and why, and what are the next steps including a timeline. By providing incentives, such as free-of-charge usage or bonus payments, users and SPs might be convinced to exploit the possibilities.

Open source and exchange: As described with the aspect integration, documentation is a must. Exchanging information and helping countries that are less developed, as with the e-Estonia Academy, lead to a higher level of maturity of eIDs and SSI worldwide. In the long run, this is a benefit for our global economy. In Denmark, the e-invoice saves taxpayers EUR 150 million a year and businesses EUR 50 million a year, while Italy's e-procurement system cuts over EUR 3 billion [157]. Due to the international economy, a worldwide-established eID ecosystem could as a result also reduce costs. With SSI, local initiatives and alliances, as in South Korea or British Columbia, may lead to successfully running systems, which then can be extended to further regions. When looking at Europe, for example, IDunion and ONCE may be a good start. Though local projects are recommended, the exchange should be worldwide, taking smaller projects such as for refugees and other use cases into account since SSI is still comparably new. By exchanging and harmonizing, interoperability may be gained.

7.1.4. Nonfunctional Factors

Security: Several identity-related incidents can occur, ranging from identity theft to data breaches. Even though SSI reduces the risk of both, the user needs to be educated and further security layers are required to to tackle, e.g., malware, ransomware, and phishing attempts. All three threats increased in 2020 rapidly [158]. When considering a privacy-preserving eID, two generic types of adversaries can be considered: (1) a malicious participant trying to forge or steal an identity, including impersonation and identity theft; (2) a malicious verifier who tries to compromise the privacy of an eID holder. The RSA key vulnerability ROCA [159] showed a dependency on chips, such as smart cards, trusted platform modules (TPM), and products using them. There may be more vulnerabilities we have not considered. The key factors for coping with the ROCA of Estonia can be repeated: using alternative solutions, which may not be affected, public private partnerships, crisis management, and documentation and verification [160]. Another important aspect is security by design [161].

Privacy: The use of personal data is strictly regulated by law. X-Road in Estonia is already one established solution. SSI is per definition centered on the user. In order to improve manageability and security, SSIs with central components were introduced. Third parties though are against the pure concept of SSI and might reduce the privacy. At the same time, it might be required for eID use cases. Running legacy systems in parallel and maybe also proxies further reduces the privacy while, at the same time, increasing the benefit and including more services and users. The challenge is finding a fitting balance. When introducing biometrics for a higher level of security, privacy may be reduced. Depending on the bootstrapping process, additional issues with privacy may occur. Even though SSI does provide a higher level of privacy, design decisions may decrease this as well.

7.1.5. Project-Specific Factors

Identification: Identification of persons, businesses, and other entities is one core element of identity management. While most European countries require ID cards or other government-issued passports, not all countries have such a law. In Japan, no ID card has been introduced at all; instead, either the driver's license or insurance card can be used. This is similar to Brazil, Canada, and the U.S., where different systems exist, depending on the state, district, and local authorities. Thereby, in the U.S., as an example, it can be more difficult to obtain an ID card if documents go missing. An SSI system may have similar problems, as creating an identity, i.e., generating a public–private key pair and an associated DID, is easy, but the process of associating the DID though verifiable credentials with an individual or organization is not standardized. Related to this is the still open question of how to build a robust system to regain control of a DID and the verifiable credentials, if they are lost or destroyed. A simple, but secure solution could be to revoke the existing verifiable credentials and start over with a new DID and new verifiable credentials. This would be similar to losing an ID card or passport, where the replacement would consist of a new passport number, but contain the same identifying information.

Harmonization: Harmonization of schemes is an enabler for interoperability. A large problem with harmonizing eIDs is the fact that different countries use diverse attributes to describe personal and organizational identities. In Latin America, migrants may have problems if the birth and host systems differ [104]. Various solutions are tried and tested in practice, such as compiling a minimal list of attributes every country must be able to provide in eIDAS, as well as schemes and attribute translation for eduGAIN. Some countries outside the EU, e.g., Azerbaijan, are eIDAS-compliant. This has the advantage that these countries mutually recognize certificates of e-signatures with European countries and, thereby, enable businesses. Even if projects are compatible at a technical level, harmonization should also consider a unified public relations and marketing strategy to prevent projects from becoming too focused on themselves and highlighting the real benefit of SSI in covering identity management in a larger ecosystem. Based on those findings, further harmonization will be needed in the future.

Trust: Trust between participating entities within the EU is provided via eIDAS, LoAs, and partly contracts. This is similar to the R&E federation eduGAIN, where different LoAs and contracts ensure the trust between participating entities. In eduGAIN, trust in the device of the user is less important than in eIDAS. Depending on the country and LoA, different forms of authentication and secure elements, e.g., software and hardware elements, within the smartphone are used. Very strict requirements provide a higher level of trust, but exclude citizens. Similar concepts to LoA are needed for SSI. Grüner et al. compared trust between FIM and SSI [162]. According to the authors, traditional identity management models have a very disparate distribution of required trust between the actors. The trust requirements with SSI are generally reduced. Nevertheless, a disparate trust distribution between the user and other entities still exists. Different approaches try to adapt the LoAs for SSI. Several directions can be seen: (1) centralized trust management infrastructure [44], (2) hybrid approaches integrating certificate authorities, (3) the Web of Trust [48], and (4) consortia such as the Digital Credentials Consortium [163]. Trust in the user is another challenge, which is currently often solved by secure elements and biometrics for authentication. An LoA may be adapted for different elements and authentication methods, lowering the burden of the user. Similar to an ID card, a smartphone can be lost. The question arises if the smartphone (resp. ID card) or the holder is authenticated.

Legislation: With different examples in classical eIDs (e.g., U.S.) and SSI (for example, South Korea), we noticed the importance of *up-to-date* regulations. When changes take longer than expected, the technical progress may come to a hold. Since politicians are typically not technically savvy persons, advisors may provide the required technical background and understanding. At the same time, processes and other aspects may need to be adapted as well.

7.2. Further Findings

When comparing the *regions* where SSI projects are prominent and the adaption of eID solutions, we noticed that SSI is especially interesting where there is either no other practical solution at all or the solution is at least not widely used. Examples for this are: Sierra Leone, homeless people in the U.S., and refugees who have no or no adequate eID solution. Comparing Germany with, e.g., Scandinavian countries or Estonia, we see that the eID acceptance is rather low, while several SSI projects are proceeding. This may have several reasons besides high security standards, which we did not explore further. We however noticed success factors: free-of-charge models for users and providers, one portal, several services including cross-sectoral, modern solutions, and high usability.

Herz and Krezdorn [55] stated that the *existence of many similar projects* in the same field is an early warning sign of potential project failure as it lowers the chances of success. When looking at Germany, this might be the case. In contrast, a like-minded peer-group, as in British Columbia, can boost the development. Turning several projects in parallel into a peer-group could lead to a successful establishment of SSI.

Complexity is the focus of several authors [52–54]. Large and/or complex projects fail more easily, while smaller projects seem to be easier to manage. As an example, introducing SSI to a city, as in Busan, or an application, as in British Columbia, and then rolling it out to further areas is more likely to succeed. The new eIDAS regulation with the addition of SSI may be more complex.

Digital *sovereignty* in Europe is one strategy, accompanied by several EU projects, such as GAIA-X, CONCORDIA, SPARTA, CyberSec4Europe, and ECHO. Sovereignty may be reached by all the SSI projects at least in this field. Nevertheless, the further evolution may lead to a dependency on private organizations and other stakeholders. The downside may not only affect countries and their citizens, but also vulnerable persons, which are dependent on having an identity.

Comparing the *maturity* of eID systems and SSI projects, we noticed several stages. The highest maturity level in all areas at the same time might not be possible however:

Location: regional, national, international;

Identification: parallel systems, nationally harmonized, internationally harmonized;

Services: core services, e-government, various services including private services;

Security: almost none, LoAs and security management, advanced backup of registries;

Usability: almost none, mobile application, easy to use multipurpose apps;

Privacy: by law, configurable including tell us once, self-sovereign.

8. Conclusions and Outlook

While classical eIDs are widely utilized, more and more SSI projects are starting. To empower users with SSI, the solution needs to obtain a significant share through adoption by users. However, users will only adopt if they see a benefit. The success factors of the eID solution in Estonia are seen in low complexity, ease of use, functionality, awareness, trust, privacy, security, control and empowerment, and transparency [15].

In order to find more factors for success and failure, we first established a taxonomy based on existing approaches and the literature. Then, we analyzed 23 eID solutions in various countries in Section 5, each with different maturity levels. We stated the features, as well as the lessons learned, limited by the information we found. This resulted in categorized lessons learned. Government-funded models help to attract additional service providers, leading to a higher benefit for the end users. While several eID solutions are built on SAML, the protocols OAuth 2.0 and OIDC help to integrate services. Documentations and published APIs again lead to easier initiation. Without users participating, eID solutions are a waste of money. Security and privacy are equally important, while LoAs provide trust among the involved entities. As different attributes are consumed in every federation or even the local system, either a minimal list of attributes (see eIDAS) or

schemes and attribute translation, as in eduGAIN, may be applied. These stated findings go beyond the success factors of Estonia.

We additionally evaluated SSI projects in twelve contexts in Section 6, which have different projects statuses, from started to deployed to terminated. Besides SSI projects targeting eID, we found projects for niches, such as the homeless and refugees. These seem more mature than classical SSI projects targeting eIDs. With legacy systems already running, bootstrapping and the transition are further challenges. In order to reach the goals, a smaller and less complex setting with enough resources is preferred. Legislation has to go hand in hand with the technical evolution. Since SSI is still evolving and we do not fully know where the journey is going, exchange is essential.

Accompanied by the status, we stated the lessons learned that we obtained from publicly available documents. Based on this analysis, we provided general lessons learned in Section 7, divided into a taxonomy and further findings. We noticed that resources and support by the top management are important factors. The technical choice should be based on the requirements, taking future situations into account. The novelty of SSI is challenging as the protocols and accompanied procedures are still being developed and improved. Therefore, technical neutrality and exchange among projects and stakeholders are major goals. IT, and thereby, identity management, is constantly evolving. Independent of the direction, classical eIDs or SSI, the underlying systems have to be updated, usable, and evolve as well. One big project is not enough: a constant effort is required.

We noticed differences in the national eID solutions. Using one solution to rule them all might not work. Nevertheless, incorporating lessons learned is advised. Interoperability among the solutions is recommended to enable international transactions and services, which is a primary goal of developments such as eIDAS. Despite having members with different cultures, eIDAS successfully uses a minimal set of attributes [164,165]. Translating attributes is another option, as can be seen in eduGAIN, which uses this solution in over 70 federations. When comparing SSI and the classical eID, pure SSI might not be desired for the eID use case. The legal and technological requirements and achievements incorporated in legacy systems need to be preserved before jumping into the next-best technological implementation. However, the integration of existing services and new solutions via proxies can be easier to achieve and pave the way toward transitioning in the long run. Whether new smartphone-based technology can improve on the usability of existing eID systems, while not incurring unacceptable security deficiencies, needs to be evaluated for each use case. Traditional identity cards also contain highly personal information and are subject to unauthorized copying, loss, and theft, and their revocation is seldom checked. The question of whether SSI is a suitable technology for (parts of) the eID use case is still unanswered. Even if it is not, having less applications on a smartphone and integrating the eID in a wallet for usability might be a suitable goal. In order to successfully enable SSI for eID use cases, exchange and an open environment are a solid base. Not solely focusing on eIDs, but also on corner cases and projects might provide a boost. In either case, the citizens' attitudes towards the solution are essential [166] to gain acceptance [167]. This might differ due to cultural differences [168,169]. Therefore, users must be involved in the development.

In future work, we will evaluate more SSI projects for different use cases in order to gain additional insights. As SSI is still a new direction, further assessments in the future will adjust the challenges and lessons learned. An analysis of LoAs based on smartphone elements and authentication methods will follow. Consequently, we will focus on the stated challenges, such as bootstrapping and revocation; see Figure 7. Furthermore, security management for SSI has to be adjusted. Last but not least, we will regard further authentication use cases, such smart and Internet of Things (IoT) devices.

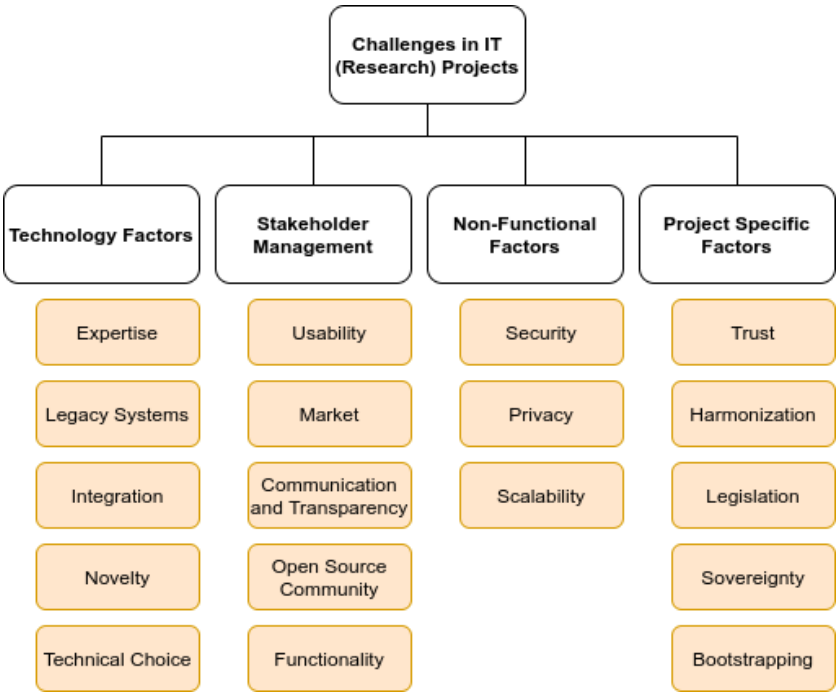

Figure 7. Challenges based on the established taxonomy.

Author Contributions: Conceptualization, D.P.; methodology, D.P.; validation, D.P., M.G. and W.H.; investigation, D.P. and M.G.; data curation, D.P.; writing—original draft preparation, D.P.; writing—review and editing, D.P., M.G. and W.H.; visualization, D.P. and M.G.; supervision, W.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work is partly funded by the Bavarian Ministry for Digital Affairs (Project DISPUT/STMD-B3-4140-1-4). The authors alone are responsible for the content of the paper.

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

References

1. European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Regulation. 2014. Available online: http://data.europa.eu/eli/reg/2014/910/oj (accessed on 11 November 2021).
2. Engelbertz, N.; Erinola, N.; Herring, D.; Somorovsky, J.; Mladenov, V.; Schwenk, J. Security Analysis of eIDAS—The Cross-Country Authentication Scheme in Europe. In Proceedings of the 12th USENIX Conference on Offensive Technologies, WOOT'18, Baltimore, MD, USA, 13–14 August 2018; USENIX Association: Berkley, CA, USA, 2018.
3. Berbecaru, D.; Lioy, A.; Cameroni, C. Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information* **2019**, *10*, 210. [CrossRef]
4. Namirial Information Technology. SPID on High Speed: State of Play on Digital Identity in Italy. 2021. Available online: https://www.namirial.com/en/namirial-spid-digital-identity-electronic-eid-italy-state-of-play-jan-2021/ (accessed on 11 November 2021).
5. PagoPA S.p.A. I Numeri dell'App IO. 2021. Available online: https://io.italia.it/dashboard (accessed on 11 November 2021).
6. Ragouzis, N.; Hughes, J.; Philpott, R.; Maler, E. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*; Specification, OASIS: Woburn, MA, USA, 2008.
7. GEANT. eduGAIN—Enabling Worldwide Access. 2021. Available online: https://edugain.org (accessed on 11 November 2021).
8. Hardt, D. The OAuth 2.0 Authorization Framework. RFC 6749, RFC Editor. 2012. Available online: http://www.rfc-editor.org/rfc/rfc6749.txt (accessed on 11 November 2021).
9. Sakimura, N.; Bradley, J.; Jones, M.B.; de Medeiros, B.; Mortimore, C. *OpenID Connect Core 1.0*; Specification, OpenID Foundation: San Ramon, CA, USA, 2014.
10. Lim, S.Y.; Fotsing, P.; Almasri, A.; Musa, O.; Mat Kiah, M.L.; Ang, T.; Ismail, R. Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735–1745. [CrossRef]
11. Toth, K.; Anderson-Priddy, A. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Secur. Priv.* **2019**, *17*, 17–27. [CrossRef]

12. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A Survey on Essential Components of a Self-Sovereign Identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
13. Cao, Y.; Yang, L. A survey of Identity Management technology. In Proceedings of the 2010 IEEE International Conference on Information Theory and Information Security, Beijing, China, 17–19 December 2010; pp. 287–293. [CrossRef]
14. Tobin, A.; Reed, D. The Inevitable Rise of Self-Sovereign Identity. 2017. Available online: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (accessed on 11 November 2021).
15. Tsap, V.; Lips, S.; Draheim, D. eID Public Acceptance in Estonia: Towards Understanding the Citizen. In Proceedings of the 21st Annual International Conference on Digital Government Research, dg.o '20, Seoul, Korea, 15–19 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 340–341. [CrossRef]
16. CEF Digital. eIDAS eID Profile. 2019. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile/ (accessed on 11 November 2021).
17. Parecki, A. OAuth 2.0. 2021. Available online: https://oauth.net/2/ (accessed on 11 November 2021).
18. Hardt, D.; Parecki, A.; Lodderstedt, T. The OAuth 2.1 Authorization Framework. Internet-Draft Draft-Ietf-Oauth-v2-1-02, IETF Secretariat. 2021. Available online: https://www.ietf.org/Internet-drafts/draft-ietf-oauth-v2-1-02.txt (accessed on 11 November 2021).
19. Richer, J.; Parecki, A.; Imbault, F. Grant Negotiation and Authorization Protocol. Internet-Draft Draft-Ietf-Gnap-Core-Protocol-06, IETF Secretariat. 2021. Available online: https://www.ietf.org/archive/id/draft-ietf-gnap-core-protocol-06.txt (accessed on 11 November 2021).
20. ISO/IEC. *ISO/IEC 29115:2013—Entity Authentication Assurance Framework*; Specification, ISO/IEC: Geneva, Switzerland, 2013.
21. Richer, J.; Johansson, L. Vectors of Trust. RFC 8485, RFC Editor. 2018. Available online: https://datatracker.ietf.org/doc/html/rfc8485 (accessed on 11 November 2021).
22. Grassi, P.A.; Garcia, M.E.; Fenton, J.L. *NIST Special Publication 800-63-3—Digital Identity Guidelines*; Specification, National Institute of Standards and Technology, U.S. Department of Commerce: Gaithersburg, ML, USA, 2017.
23. Drummond, R.; Manu, S.; Dave, L.; Markus, S.; Christopher, A.; Orie, S. Decentralized Identifiers (DIDs) v1.0. Proposed Recommendation. 2021. Available online: https://www.w3.org/TR/did-core/ (accessed on 11 November 2021).
24. Tobin, A.; Reed, D.; Windley, P.J. *The Inevitable Rise of Self-Sovereign Identity*; The Sovrin Foundation: Provo, UT, USA, 2016; pp. 1–23.
25. Windley, P. The Sovrin SSI Stack. 2020. Available online: https://www.windley.com/archives/2020/03/the_sovrin_ssi_stack.shtml (accessed on 11 November 2021).
26. Hyperledger White Paper Working Group. *An Introduction to Hyperledger*; Linux Foundation: San Fransisco, CA, USA, 2018.
27. George, N. Announcing Hyperledger Aries, Infrastructure Supporting Interoperable Identity Solutions! 2019. Available online: https://www.hyperledger.org/blog/2019/05/14/announcing-hyperledger-aries-infrastructure-supporting-interoperable-identity-solutions (accessed on 11 November 2021).
28. Lesavre, L.; Varin, P.; Mell, P.; Davidson, M.; Shook, J. *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*; Whitepaper NIST: Gaithersburg, ML, USA, 2020. [CrossRef]
29. Kubach, M.; Sellung, R. On the Market for Self-Sovereign Identity: Structure and Stakeholders. In *Open Identity Summit 2021*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2021; pp. 143–154.
30. Carretero, J.; Izquierdo-Moreno, G.; Vasile-Cabezas, M.; Garcia-Blas, J. Federated Identity Architecture of the European eID System. *IEEE Access* **2018**, *6*, 75302–75326. [CrossRef]
31. Kuperberg, M.; Kemper, S.; Durak, C. Blockchain Usage for Government-Issued Electronic IDs: A Survey. In *Advanced Information Systems Engineering Workshops*; Proper, H.A., Stirna, J., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 155–167.
32. Federal Ministry for Economic Affairs and Energy. Showcase Programme "Secure Digital Identities". 2021. Available online: https://www.digitale-technologien.de/DT/Navigation/EN/Foerderprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (accessed on 11 November 2021).
33. Gilb, C. Zukunft der Zuger Digitalen ID Ist Ungewiss. 2019. Available online: https://www.luzernerzeitung.ch/zentralschweiz/zug/zukunft-der-digitalen-id-ist-ungewiss-ld.1163192 (accessed on 11 November 2021).
34. Danish, M.S.S.; Yona, A.; Senjyu, T. Insights Overview of Afghanistan Electronic National Identification Documents: eGovernment, eID Card, and ePassport Schemes. In Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 1–3 September 2014; pp. 251–255. [CrossRef]
35. Berbecaru, D.; Lioy, A. On the design, implementation and integration of an Attribute Provider in the Pan-European eID infrastructure. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016; pp. 1263–1269. [CrossRef]
36. Quiroz, E.P.; Cuno, A.; Sarmiento, E.; Cruzado, E. Requirements for a new Peruvian electronic identity card. In Proceedings of the 2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, Peru, 3–5 September 2020; pp. 1–4. [CrossRef]
37. Lenz, T.; Alber, L. Towards Cross-Domain eID by Using Agile Mobile Authentication. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 1–4 August 2017; pp. 570–577. [CrossRef]

38. Zefferer, T.; Ziegler, D.; Reiter, A. Best of two worlds: Secure cloud federations meet eIDAS. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 396–401. [CrossRef]
39. Burgstaller, L.; Gaggl, B.; Koch, K.M.; Leitold, H.; Teufl, P.; Zefferer, T.; Hühnlein, D.; Hammer, S.; Corici, A.A.; Lampoltshammer, T.; et al. D1.1.—Survey of Related Work. Deliverable, mGov4EU. 2021. Available online: https://www.mgov4.eu/fileadmin/mgov-files/pub/mGov4EU-D1.1-PU-M03-website.pdf (accessed on 11 November 2021).
40. Dib, O.; Toumi, K. Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. In *Annals of Emerging Technologies in Computing (AETiC)*; International Association of Educators and Researchers (IAER): Wrexham, UK, 2020; Volume 4, pp. 19–40. [CrossRef]
41. Kubach, M.; Schunck, C.H.; Sellung, R.; Roßnagel, H. Self-sovereign and Decentralized identity as the future of identity management? In *Open Identity Summit 2020*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Hühnlein, D., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2020; pp. 35–47. [CrossRef]
42. Vila, X. SSI eIDAS Bridge Project: ESSIF-Lab/Infrastructure/VALIDATED-ID/SEB Project Summary. 2021. Available online: https://gitlab.grnet.gr/essif-lab/infrastructure/validated-id/seb_project_summary (accessed on 11 November 2021).
43. eSSIF-LAB. NGI eSSIF-LAB—European Self-Sovereign Identity Framework Lab. 2021. Available online: https://essif-lab.eu (accessed on 11 November 2021).
44. Kubach, M.; Roßnagel, H. A lightweight trust management infrastructure for self-sovereign identity. In *Open Identity Summit 2021*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2021; pp. 155–166.
45. LIGHTest. 2019. Available online: https://www.lightest.eu/ (accessed on 11 November 2021).
46. Alber, L.; More, S.; Mödersheim, S.; Schlichtkrull, A. Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World. In *Open Identity Summit 2021*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2021; pp. 107–118.
47. Martinez Jurado, V.; Vila, X.; Kubach, M.; Henderson Johnson Jeyakumar, I.; Solana, A.; Marangoni, M. Applying assurance levels when issuing and verifying credentials using Trust Frameworks. In *Open Identity Summit 2021*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2021; pp. 167–178.
48. Brunner, C.; Gallersdörfer, U.; Knirsch, F.; Engel, D.; Matthes, F. DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications, Xi'an, China, 14–16 September 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 61–66.
49. Aragó-Monzonís, F.J.; Domínguez-García, L.; Basurte-Durán, A.; Ocana, R.; Giralt, V. SEAL Project: User-centric Application of Linked Digital Identity for Students and Citizens. In Proceedings of the ICDS 2020, Fourteenth International Conference on Digital Society, Valencia, Spain, 21–25 November 2020; pp. 108–111.
50. Abraham, A.; Hörandner, F.; Omolola, O.; Ramacher, S. Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems. In *Information and Communications Security*; Zhou, J., Luo, X., Shen, Q., Xu, Z., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 307–323.
51. Stokkink, Q.; Epema, D.H.J.; Pouwelse, J. A Truly Self-Sovereign Identity System. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 1–8. [CrossRef]
52. Al-Ahmad, W.; Al-Fagih, K.; Khanfar, K.; Alsamara, K.; Abuleil, S.; Abu-Salem, H. A Taxonomy of an IT Project Failure: Root Causes. *Int. Manag. Rev.* **2009**, *5*, 93–104.
53. Whitney, K.M.; Daniels, C.B. The Root Cause of Failure in Complex IT Projects: Complexity Itself. *Procedia Comput. Sci.* **2013**, *20*, 325–330. [CrossRef]
54. Chapman, P.; Quang, C. *Major Project Risk Management: Reconciling Complexity during Delivery with the Inside View in Planning*; Center for Open Science: Oxford, UK, 2021. [CrossRef]
55. Herz, M.; Krezdorn, N. Epic fail: Exploring project failure's reasons, outcomes and indicators. *Rev. Manag. Sci.* **2021**, 1–25. [CrossRef]
56. European Commission. Digital Government Factsheet 2019—Norway. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Norway_2019.pdf (accessed on 11 November 2021).
57. Signicat. Norwegian BankID. 2021. Available online: https://developer.signicat.com/enterprise/identity-methods/norwegian-bankid.html (accessed on 11 November 2021).
58. Digdir Docs. Docs. 2021. Available online: https://docs.digidr.no/index.html (accessed on 11 November 2021).
59. Vipps AS. Services—BankID. 2021. Available online: https://www.bankid/en/about-us/services/ (accessed on 11 November 2021).
60. European Commission. Digital Government Factsheet 2019—Sweden. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Sweden_2019.pdf (accessed on 11 November 2021).
61. European Commission. Digital Government Factsheet 2019—Finland. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Finland_2019.pdf (accessed on 11 November 2021).
62. Digital Iceland. IceKey. 2021. Available online: https://island.is/en/icekey (accessed on 11 November 2021).

63. Nazario, J. *Political DDoS: Estonia and Beyond*; USENIX Association: San Jose, CA, USA, 2008.
64. e-Estonia. Security and Safety. 2019. Available online: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/ (accessed on 11 November 2021).
65. European Commission. Digital Government Factsheet 2019—Estonia. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Estonia_2019.pdf (accessed on 11 November 2021).
66. Eichholtzer, M.; Kirova, M. Overview of Pre-Notified and Notified eID Schemes under eIDAS. 2021. Available online: http://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (accessed on 11 November 2021).
67. European Commission. Digital Government Factsheet 2019—Latvia. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Latvia_2019.pdf (accessed on 11 November 2021).
68. European Commission. Digital Government Factsheet 2019—Lithuania. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Lithuania_2019.pdf (accessed on 11 November 2021).
69. eGA. e-Governance Academy. 2021. Available online: https://ega.ee (accessed on 11 November 2021).
70. Egovernment—Schweiz Suisse Svizzera. Implementing eID. 2021. Available online: https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat/ (accessed on 11 November 2021).
71. Digitales Österreich. Mobile Phone Signature & Citizen Card—The Electronic ID. 2021. Available online: https://www.buergerkarte.at/en/ (accessed on 11 November 2021).
72. Federal Office for Information Security. German eID. 2021. Available online: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/german-eID_node.html (accessed on 11 November 2021).
73. BDR. OPTIMOS—A Practical Ecosystem of Secure Identities for Mobile Services. 2021. Available online: https://www.bundesdruckerei.de/en/innovations/optimos (accessed on 11 November 2021).
74. Bundesministerium des Innern, für Bau und Heimat. Das Projekt Digitale Identitäten. 2021. Available online: https://www.personalausweisportal.de/Webs/PA/DE/verwaltung/projekt_digitale_identitaeten/projekt_digitale_identitaeten_node.html (accessed on 11 November 2021).
75. Governikus, K.G. AusweisApp2. 2021. Available online: https://www.ausweisapp.bund.de/en/ausweisapp2-home/ (accessed on 11 November 2021).
76. CSAM. eID Software. 2021. Available online: https://eid.belgium.be/en (accessed on 11 November 2021).
77. Belgian Mobile ID SA/NV. Discover Itsme. 2021. Available online: https://www.itsme.be/en/ (accessed on 11 November 2021).
78. Het Facilitair Bedrijf for the Flemish Government. About Identity and Access Management Platform of the Flemish Government. 2021. Available online: https://joinup.ec.europa.eu/collection/eidentity-and-esignature/solution/identity-and-access-management-platform-flemish-government/about (accessed on 11 November 2021).
79. European Commission. Digital Government Factsheet 2019—France. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_France_2019.pdf (accessed on 11 November 2021).
80. République Française. FranceConnect. 2021. Available online: https://github.com/france-connect (accessed on 11 November 2021).
81. European Commission. Digital Government Factsheet 2019—Italy. Report. European Commission. 2019. Available online: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Italy_2019.pdf (accessed on 11 November 2021).
82. Dipartimento per la Transformazione Digitale + AgID. CIE Eletronic Identity Card. 2021. Available online: https://developers.italia.it/en/cie (accessed on 11 November 2021).
83. Agenzia per l'italia Digitale. SPID Public Digital Identity System. 2021. Available online: https://www.spid.gov.it/en (accessed on 11 November 2021).
84. AMA Portugal. The Portuguese Digital Identity Ecosystem. 2021. Available online: https://joinup.ec.europa.eu/collection/portuguese-egovernment-solutions/news/portugals-pioneering-eid-solutions (accessed on 11 November 2021).
85. Smart Dubai. Smart Dubai. 2021. Available online: https://www.smartdubai.ae (accessed on 11 November 2021).
86. Afifi, M.A.M. Insights on National Identity Cards Potential Applications and Digitizing Its Uses Based on the EID Card. In Proceedings of the 2019 International Conference on Digitization (ICD), Sharjah, United Arab Emirates, 18–19 November 2019; pp. 160–166. [CrossRef]
87. Identity Review. UAE Invests Early in Digital Identity and Blockchain, Pays off during COVID-19 Pandemic. 2020. Available online: https://identityreview.com/uae-invests-early-in-digital-identity-and-blockchain/ (accessed on 11 November 2021).
88. Marri, A.A.; Albloosh, F.; Moussa, S.; Elmessiry, H. Study on The Impact of Artificial Intelligence on Government E-service in Dubai. In Proceedings of the 2019 International Conference on Digitization (ICD), Sharjah, United Arab Emirates, 18–19 November 2019; pp. 153–159. [CrossRef]
89. Ministry of Transport, Communication and Information Technology. National Digital Certification Center. 2021. Available online: https://oman.om/tam/ (accessed on 11 November 2021).

90. National Identity Management Commission. MWS NIMC Mobile Identity. 2021. Available online: https://nimcmobile.app (accessed on 11 November 2021).
91. National Identity Management Commission. Fraud Alert. 2021. Available online: https://nimc.gov.ng/fraud-alert/ (accessed on 11 November 2021).
92. Okunoye, B. Nigeria: There Can Be No Digital Identity (ID) without Digital Security. 2021. Available online: https://www.africaportal.org/features/nigeria-there-can-be-no-digital-identity-id-without-digital-security/ (accessed on 11 November 2021).
93. Government of Singapore. SingPass. 2021. Available online: https://www.singpass.gov.sg/main (accessed on 11 November 2021).
94. Gibson, R.; Ward, S.J.; Chen, P.; Lusoli, W. Australian Government and Online Communication. In *Government Communication in Australia*; Young, S., Ed.; Cambridge University Press: Cambridge, UK, 2007; pp. 161–180.
95. Hanson, G.; Ott, A.; Krenjova, J. Introducing Integrated E-Government in Australia. 2018. Available online: https://www.acs.org.au/content/dam/acs/acs-publications/E-Gov%20Report.pdf (accessed on 11 November 2021).
96. Greenleaf, G. The Australia Card: Towards a National Surveillance System. *Law Soc. J.* **1987**, *25*, *1–14*.
97. Australian Government. Trusted Digital Identity Framework. 2019. Available online: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework (accessed on 11 November 2021).
98. Australian Postal Cooperation. Digital iD—ID on Your Phone. 2019. Available online: https://www.digitalid.com (accessed on 11 November 2021).
99. Coalition, T.B.I. Five Key Initiatives. 2018. Available online: https://www.betteridentity.org/five-key-initiatives (accessed on 11 November 2021).
100. Social Security. Social Security: Fraud Prevention and Reporting. 2021. Available online: https://www.ssa.gov/fraud (accessed on 11 November 2021).
101. Otto, G. NCIST Gives $15M in Grants for Identity Management Pilots. 2016. Available online: https://statescoop.com/nstic-gives-15m-in-grants-for-identity-management-pilots/ (accessed on 11 November 2021).
102. ADOT. Mobile ID. 2021. Available online: https://azdot.gov/motor-vehicles/driver-services/mobile-id (accessed on 11 November 2021).
103. Greenwood, D. Wyoming Digital Identity Legislation Update. 2020. Available online: https://civics.com/2020/09/29/wyoming-digital-identity-legislation-update/ (accessed on 11 November 2021).
104. Pivcevic, K. Challenges in Latin American Biometric National ID Initiatives Outlined by Women in Identity. 2020. Available online: https://www.biometricupdate.com/202011/challenges-in-latin-american-biometric-national-id-initiatives-outlined-by-women-in-identity (accessed on 11 November 2021).
105. de Kalaf, E.H. How Some Countries Are Using Digital ID to Exclude Vulnerable People around the World. 2021. Available online: https://theconversation.com/how-some-countries-are-using-digital-id-to-exclude-vulnerable-people-around-the-world-164879 (accessed on 11 November 2021).
106. andina. DNI Electrónico gana Premio al Mejor Documento de Identificación de América Latina. 2015. Available online: https://andina.pe/agencia/noticia-dni-electronico-gana-premio-al-mejor-documento-identificacion-america-latina-562655.aspx (accessed on 11 November 2021).
107. Mason, O. Brazil 'Champion' in Card Fraud, with 45.4% of Global Cases—Report. 2021. Available online: https://riotimesonline.com/brazil-news/brazil/brazil-champion-in-card-fraud-with-45-4-of-global-cases/ (accessed on 11 November 2021).
108. Belli, L. The Largest Personal Data Leakage in Brazilian History. 2021. Available online: https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/ (accessed on 11 November 2021).
109. The Lancet. The unfolding migrant crisis in Latin America. *Lancet* **2019**, *394*, 1966. [CrossRef]
110. Khoury, N. *Digital Identity: Enabling Dignified Access to Humanitarian Services in Migration*; Report; International Federation of Red Cross and Red Crescent Societies: Geneva, Switzerland, 2021.
111. McGibbon, A. *Review of the Events Surrounding the 2016 eCensus*; Technical Report; Australian Government—Office of the Cyber Security Special Adviser: Canberra, Australia, 2016.
112. Information Commissioner's Office. ICO Fines Marriott International Inc £18.4million for Failing to Keep Customers' Personal Data Secure. 2020. Available online: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/ (accessed on 11 November 2021).
113. ForgeRock. *2021 ForgeRock Consumer Identity Breach Report—Pandemic Exacerbates Vulnerabilities Created by Years of Cybersecurity Complacency*; Breach Report; ForgeRock: San Francisco, CA, USA, 2021.
114. Sportiello, L. "Internet of Smart Cards": A pocket attacks scenario. *Int. J. Crit. Infrastruct. Prot.* **2019**, *26*, 100302. [CrossRef]
115. Rashid, N. *Deploying the Once-Only Policy: A Privacy-Enhancing Guide for Policymakers and Civil Society Actors*; Report; Harvard Kennedy School—Ash Center for Democratic Governance and Innovation: Cambridge, MA, USA, 2020.
116. Krimmer, R.; Prentza, A.; Mamrot, S.; Schmidt, C. The Once-Only Principle: A Matter of Trust. In *The Once-Only Principle: The TOOP Project*; Krimmer, R., Prentza, A., Mamrot, S., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 1–8. [CrossRef]
117. Schmidt, C.; Krimmer, R.; Lampoltshammer, T. *"When Need Becomes Necessity"—The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View*; Zenodo: Bonn, Germany, 2021. [CrossRef]

118. Pöhn, D.; Hommel, W. Automated User Information Conversion to improve Identity Federation Scalability. In Proceedings of the 22th Congress of the European University Information Systems Organisation (EUNIS 2016), Thessaloniki, Greece, 2016. Available online: https://docplayer.net/23435729-Automated-user-information-conversion-to-improve-identity-federation-scalability.html (accessed on 16 November 2021).
119. European Commission. Digital Identity and Trust: Commission Launches Public Consultation on the eIDAS Regulation. 2020. Available online: https://docplayer.net/23435729-Automated-user-information-conversion-to-improve-identity-federation-scalability.html (accessed on 11 November 2021).
120. KRAKEN. The Project Kraken. 2021. Available online: https://www.krakenh2020.eu/the_project/overview (accessed on 11 November 2021).
121. mGov4EU. mGov4EU Project. 2021. Available online: https://www.mgov4.eu (accessed on 11 November 2021).
122. CONCORDIA. CONCORDIA. 2021. Available online: https://www.concordia-h2020.eu (accessed on 11 November 2021).
123. CEF Digital. EBSI—Experience the Future with the European Blockchain Services Infrastructure (EBSI). 2021. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (accessed on 11 November 2021).
124. IDunion. IDunion—Enables Self-Determined Identities. 2021. Available online: https://idunion.org/?lang=en (accessed on 11 November 2021).
125. ONCE. ONCE Project. 2021. Available online: https://www.once-project.de (accessed on 11 November 2021).
126. BDR. *From the Almighty Administrator to the Self-Determined User*; Whitepaper: Berlin, Germany, 2018.
127. Lissi. Lissi—Identity Wallet and Identity Management Solution. 2021. Available online: https://lissi.id/start (accessed on 11 November 2021).
128. Otte, P.; de Vos, M.; Pouwelse, J. TrustChain: A Sybil-resistant scalable blockchain. *Future Gener. Comput. Syst.* **2020**, *107*, 770–780. [CrossRef]
129. Pouwelse, J. Towards the Science of Essential Decentralised Infrastructures. In Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good, DICG'20, Online, 7–11 December 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–6. [CrossRef]
130. Stokkink, Q.; Pouwelse, J. Deployment of a Blockchain-Based Self-Sovereign Identity. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1336–1342. [CrossRef]
131. Flemish Government. Blockchain on the Move (BotM). 2021. Available online: https://www.innovatieveoverheidsopdrachten.be/en/projects/blockchain-move-botm (accessed on 11 November 2021).
132. DIZME. Dizme. 2021. Available online: https://www.dizme.io (accessed on 11 November 2021).
133. Trust over IP Foundation. *Introducing the Trust over IP Foundation*; Whitepaper: San Francisco, CA, USA, 2020.
134. Kiva. Kiva Protocol—Building the Credit Bureau of the Future. 2018. Available online: https://www.kiva.org/protocol (accessed on 11 November 2021).
135. Wang, F.; De Filippi, P. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Front. Blockchain* **2020**, *2*, 1–22. [CrossRef]
136. Cheesman, M.; Slavin, A., Self-sovereign identity and forced migration: Slippery terms and the refugee data apparatus. In *Digital Identity, Virtual Borders and Social Media*; Edward Elgar Publishing: Cheltenham, UK, 2021; pp. 10–32.
137. Rohingya Project. Rohingya Project—Financial and Social Inclusion Platform for Stateless—Digitally Empowering Stateless. 2021. Available online: https://rohingyaproject.com (accessed on 11 November 2021).
138. Gadnis, A. Opinion: Blockchain Offers Poorest a Real Economic Identity—And a Shot at the SDGs. 2016. Available online: https://www.devex.com/news/opinion-blockchain-offers-poorest-a-real-economic-identity-and-a-shot-at-the-sdgs-89071 (accessed on 11 November 2021).
139. Cheesman, M. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics* **2020**, 1–26. [CrossRef]
140. Coinplug. Busan Blockchain Regulation-Free Zone Project. 2021. Available online: https://coinplug.com/EN/busan (accessed on 11 November 2021).
141. British Columbia. British Columbia's Verifiable Organizations. 2021. Available online: https://orgbook.gov.bc.ca/en/home (accessed on 11 November 2021).
142. BCDevExchange. BCDDevExchange. 2021. Available online: https://bcdevexchange.org (accessed on 11 November 2021).
143. Hyperledger Foundation. *Case Study: BC Aims to Cut Government Red Tape with Hyperledger Indy*; Hyperledger Foundation: San Francisco, CA, USA, 2019.
144. British Columbia. Province of British Columbia. 2021. Available online: https://github.com/bcgov (accessed on 11 November 2021).
145. National Alliance to End Homelessness. State of Homelessness: 2021 Edition. 2021. Available online: https://endhomelessness.org/homelessness-in-america/homelessness-statistics/state-of-homelessness-2021/ (accessed on 11 November 2021).
146. Iyengar, R.; Albert, J. *California Blockchain Working Group—Digital Identity*; Report; State of California: Sacramento, CA, USA, 2020.
147. Mercer, T.; Khurshid, A. Advancing Health Equity for People Experiencing Homelessness Using Blockchain Technology for Identity Management: A Research Agenda. *J. Health Care Poor Underserved* **2021**, *32*, 262–277. [CrossRef]

148. Khurshid, A.; Rajeswaren, V.; Andrews, S. Using Blockchain Technology to Mitigate Challenges in Service Access for the Homeless and Data Exchange Between Providers: Qualitative Study. *J. Med. Internet Res.* **2020**, *22*, e16887. [CrossRef] [PubMed]
149. Blockchain for Change. FUMMI—Blockchain Smart ID and Alternative Financial Services. 2021. Available online: https://blockchainforchange.org/fummi (accessed on 11 November 2021).
150. City of Austin. Github—MyPass Project. 2021. Available online: https://github.com/cityofaustin/mypass-project (accessed on 11 November 2021).
151. DOIT—Illinois Department of Innovation & Technology. Blockchain in Illinois. 2021. Available online: www2.illinois.gov/sites/doit/pages/BlockChainInitiative.aspx (accessed on 11 November 2021).
152. LACChain. LACChain. 2021. Available online: https://www.lacchain.net/home?lang=en (accessed on 11 November 2021).
153. Preukschat, A.; Carmona, L.; Paramo, D. *The Ecosystem of Decentralised Digital Identity in the Spanish and Portuguese Speaking World*; Report; Blockchain Espana and SSIMeetup. 2020. Available online: https://www.ssimeetup.org//latam-spain-identity/ (accessed on 11 November 2021).
154. Maram, D.; Malvai, H.; Zhang, F.; Jean-Louis, N.; Frolov, A.; Kell, T.; Lobban, T.; Moy, C.; Juels, A.; Miller, A. CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), Online, 24–27 May 2021; IEEE Computer Society: Los Alamitos, CA, USA, 2021; pp. 1348–1366. [CrossRef]
155. Zhang, F.; Maram, D.; Malvai, H.; Goldfeder, S.; Juels, A. DECO: Liberating Web Data Using Decentralized Oracles for TLS. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, CCS '20, Online, 9–13 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1919–1938. [CrossRef]
156. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
157. European Commission. eGovernment and Digital Public Services. 2021. Available online: https://digital-strategy.ec.europa.eu/en/policies/egovernment (accessed on 11 November 2021).
158. Brooks, C. Alarming Cybersecurity Stats: What You Need to Know for 2021. 2021. Available online: https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/ (accessed on 11 November 2021).
159. Nemec, M.; Sys, M.; Svenda, P.; Klinec, D.; Matyas, V. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, Dallas, TX, USA, 30 October–3 November 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1631–1648. [CrossRef]
160. Lips, S.; Pappel, I.; Tsap, V.; Draheim, D. Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field. In *Electronic Government and the Information Systems Perspective*; Kő, A., Francesconi, E., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 60–70.
161. Oruaas, M.; Willemson, J. Developing Requirements for the New Encryption Mechanisms in the Estonian eID Infrastructure. In *Databases and Information Systems*; Robal, T., Haav, H.M., Penjam, J., Matulevičius, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 13–20.
162. Grüner, A.; Mühle, A.; Gayvoronskaya, T.; Meinel, C. A Comparative Analysis of Trust Requirements in Decentralized Identity Management. In *Advanced Information Networking and Applications*; Barolli, L., Takizawa, M., Xhafa, F., Enokido, T., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 200–213.
163. Chartrand, J.; Freeman, S.; Gallersdörfer, U.; Lisle, M.; Mühle, A.; van Engelenburg, S. *Building the Digital Credential Infrastructure for the Future*; Whitepaper. 2020. Available online: https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf (accessed on 11 November 2021).
164. Kubicek, H.; Noack, T. Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity Inf. Soc.* **2010**, *3*, 235–245. [CrossRef]
165. Brugger, J.; Fraefel, M.; Riedl, R. Raising Acceptance of Cross-Border eID Federation by Value Alignment. *Electron. J. Gov.* **2014**, *12*, 179–199.
166. Axelsson, K.; Melin, U. *Citizens' Attitudes towards Electronic Identification in a Public E-Service Context—An Essential Perspective in the eID Development Process*; Electronic Government; Scholl, H.J., Janssen, M., Wimmer, M.A., Moe, C.E., Flak, L.S., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 260–272.
167. Tsap, V.; Pappel, I.; Draheim, D. Factors Affecting e-ID Public Acceptance: A Literature Review. In Proceedings of the International Conference on Electronic Government and the Information Systems Perspective, Bratislava, Slovakia, 14–17 September 2019; Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 176–188.
168. Wallis, C.; McKenzie, R.; Crompton, M. Use Cases for Identity Management in E-Government. *IEEE Secur. Priv.* **2008**, *6*, 51–57. [CrossRef]
169. van Dijck, J.; Jacobs, B. Electronic identity services as sociotechnical and political-economic constructs. *New Media Soc.* **2020**, *22*, 896–914. [CrossRef]