H. Roßnagel, C. H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 167

Applying assurance levels when issuing and verifying credentials using Trust Frameworks

Victor Martinez Jurado[1], Xavier Vila[2], Michael Kubach[3], Isaac Henderson Johnson Jeyakumar[3], Albert Solana[2], Matteo Marangoni[1]

Abstract: Technical interoperability of the issuance, presentation, and verification of verifiable credentials (VC) across domains of trust is a current challenge for self-sovereign identity. We present an approach incorporating different levels of assurance and trust domains in an eIDAS compliant way. This is illustrated through a use case with real-world relevance: the issuance and cross-border usage of the European Health Insurance Card.

Keywords: eIDAS, self-sovereign identity, SSI, trust, trust frameworks, verifiable credentials

1 Introduction

When providing electronic services in a cross-border context, providers should have in place practices, policies, and other controls to provide assurance and evidence to the governor bodies of different trust schemes that effective practices are in place. The whole ecosystem benefits from this practice since consumers (holders, verifiers) can rely on the authorities and on the applied trust schemes to provide the needed assurance on the services consumed. The eIDAS regulation [Eu14] provides a such framework for determining the assurance levels of electronic identification schemes. However, eIDAS is focused on the EU, while many other domains of trust exist and even more could be defined. Hence, it would be advantageous if individuals or groups (industry organizations, NGOs, etc.) of verifiers could define for themselves their required trust standards and refer to self-defined trust schemes or schemes defined by other trustable entities besides the EU.

This paper describes the concept jointly developed by SICPA, Validated ID, and Fraunhofer in the EU NGI ESSIF Lab [ES21], demonstrating the issuance, presentation, and verification of verifiable credentials (VC), incorporating different domains of trust. Firstly, we demonstrate how we can leverage the SSI-eIDAS Bridge to provide legal confirmation of the identity of the issuer (using a Qualified Electronic Certificate) and a legal basis for attributing a VC to an issuer (by using electronic seals); and secondly, we propose the TRAIN approach as means to verify that an issuer was authoritative to issue a VC (by integration in a trust scheme infrastructure) so it can be trusted by the verifier. The use case chosen to illustrate this concept is the European Health Insurance Card.

[1] SICPA SA, Av. de Florissant 41, 1008 Prilly, Switzerland, firstname.lastname@sicpa.com
[2] Validated ID, C/ Aragó 179, 08011 Barcelona, Spain, firstname.lastname@validated.id
[3] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, Germany, firstname.lastname@iao.fraunhofer.de

The concept combines the following building blocks: (1) An interoperable issuance, presentation, and verification application that can support multiple protocols, credential types, and did-methods. (2) An SSI-eIDAS bridge component, providing legal confirmation of the identity of the issuer by incorporating the Issuer's advanced or qualified electronic signature or seal. (3) A Trust Management Infrastructure (TRAIN), providing a globally applicable means to verify conformance of the issuer to a certain policy and trusted scheme, fostering the trustworthiness of the electronic transaction.

The paper is structured as follows. Chapter 2 presents the EHIC use case that illustrates our approach. Subsequently, chapter 3 depicts the generic solution architecture with its elements. Chapters 4, 5, and 6 give details on our main components: the SICPA Bridge, the SSI-eIDAS Bridge and the TRAIN infrastructure. Finally, we come to a conclusion, point at open issues and lay down our next steps in chapter 7.

2 The European Health Insurance Card (EHIC) use-case

The problem: The EHIC scheme allows EU citizens to obtain free medical care or in some cases at a local rate if they are visiting countries that take part in the scheme [Eu21]. The EHIC scheme covers emergency treatment and certain pre-existing medical conditions. EHIC fraud occurs when visitors claim for treatments under EHIC when they are not entitled to do so. The main fraud types in this category are (1) False Application: This relates to someone who has intentionally made a fraudulent application for a European Health Insurance Card, and (2) False Use: This relates to someone using a European Health Insurance Card who has no entitlement to do so.

High-level approach: We would like to leverage the eIDAS framework to provide a substantial assurance level on the issuer's identity, both when holders and verifiers receive and validate the EHIC credential or presentation. We regard VCs as an appropriate technology for the use case, as it provides flexibility and decentralization. First, enhance the trust between issuers, holders, and verifiers, secondly solve the Just in time issuance problem in Identity systems (verifier no longer has to contact the issuer). Citizens (holders) can keep control and ownership over their digital EHIC, deciding what information they want to disclose, sharing only the required data to whom they wish to disclose it. (currently, various available cryptography techniques can be used to achieve selective disclosure or data minimization, i.e. Zero-Knowledge Proofs). At the same time, we want to minimize false use by applying different trust frameworks (private health insurance providers as valid issuers, holder-specific entitlements, etc) on the verification of the EHIC credential and related entitlements.

Goals: The goals of our approach are to (1) demonstrate the issuance of EHIC by health insurance providers, applying eIDAS framework, (2) demonstrate the verification of EHIC by cross-border healthcare providers to ensure entitlements are valid, and (3) apply country/healthcare specific trust frameworks to ensure false use is mitigated.

Stakeholders, Roles, and Components: The following table (*Figure 1*) gives an overview of the relevant stakeholders and their roles in our exemplary use case, mapped to the components of our solution architecture.

Stakeholders	Role	Component
National Health Insurance Provider	Issuer of EHIC, issuer of entitlements, payer	Issuance service, SSI-eIDAS bridge
Healthcare provider	Verifier of EHIC, provider of service, payee	Verification service, TRAIN ATV, SSI-eIDAS bridge
Citizen	Holder, consumer of healthcare service	Wallet
National Government	Accreditation of National Health Insurance Providers	TRAIN TPA
EU	Provides trust framework for cross-border usage of EHIC	TRAIN TSPA

Figure 1: Stakeholders, Roles, Components

3 Architecture

Our architecture defines the following components, while Figure *2* below gives a high-level, generic overview of the intended architecture context for this concept.

A) Holder/Wallet: This is the software that is able to request/store/manage the user's VCs, and possibly related artifacts such as DIDs and cryptographic keys.

B) Issuance application backend: Logic associated with preparing VC data for a Holder with issuing credentials.

C) Issuance application backend Front-end: Renders to the user's agent software, helping them obtain the credential and navigate the Issuer business logic.

D) VC Issuer HTTP API Service: An implementation of the VCs Issuer HTTP API that is capable of generating VCs with a qualified electronic seal attached to it.

E) Verification application backend Front-end: Renders to the user's agent software, requesting them a Verifiable presentation and navigating the Verifier business logic.

F) VC Verification HTTP API Service: An implementation of the VCs Verifier HTTP API that is capable of verifying VCs / Presentation, verifying qualified electronic seals, and verifying conformance of the issuer to a certain policy and trusted scheme.

G) SSI-eIDAS bridge: Enhance the legal certainty of the VC issued, by incorporating the issuer’s advanced or qualified electronic seal. For details see chapter 4.

H) TRAIN: Provides a global trust infrastructure that can be used to verify conformance of the issuer to a certain policy and trusted scheme. For details see chapter 5.

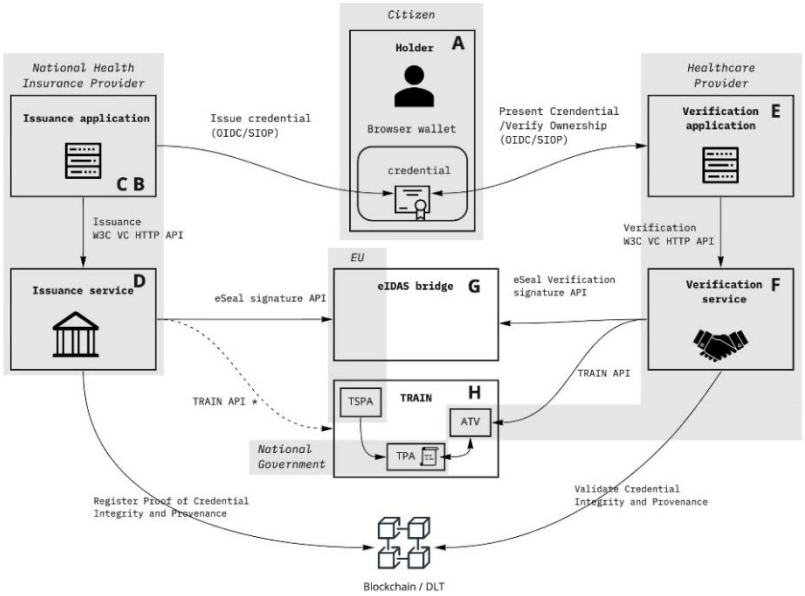

Figure 2: Proposed Architecture and with Stakeholders

3.1 Scope and Process

In order to achieve practical interoperability and build an end-to-end use-case from issuance to verification, the scope of the work has been limited. The VC-data model [VR20] is rendered using [JSON-LD] with the usage of linked data proofs [LD-PROOF] [Li20a]. The protocol used to transfer credentials between issuer - wallet - verifier is OIDC (see more details 3.3 Connectors). The scope of TRAIN in this use case is to verify whether a certain Credential Issuer (identified via DID) is enrolled in a certain Trust Scheme (identified via DNS Hostname) as required by the Verifier in a Verifier Policy. Both, the enrolment process of the issuer in the Trust Scheme, as well as the formulation of a (dynamic) Verifier Policy are for now out of the scope of this concept. Finally, did:key is the only did method supported in this use-case. The process is as follows:

1. Enrolment of the Issuer as a Trust Schema member by a Trust Scheme Operator (Trust Scheme Publication Authority or Trust Publication Authority) via Train (out of the scope of this current version, manual installation step)
2. Holder connects with the Issuer and requests a credential via OpenID.
3. Holder authenticates with his wallet, using it as a Self-Issued OpenID provider.
4. Issuer generates credential, signs and e-seals it, and sends to wallet back via OpenID.
5. Presentation Request by the Verifier to the wallet using OIDC.
6. Presentation Submission to the Verifier website by the wallet using OIDC.

7. Cryptographic Verification of the presentation by Verifier.
8. Verification of the seal by SSI-eIDAS bridge.
9. Verification of conformance of the issuer to a certain policy that is defined by the verifier through check of integration in a certain trusted scheme by TRAIN.

3.2 European Health Insurance Card Vocabulary Specification

For this concept, we have specified a Linked Data vocabulary for asserting VCs related to European Health Insurance Card (EHIC) information, such as Insurance number, Country, ID number of the insurance carrier. It is published at [MM21].

3.3 Connectors

We are using OpenID to connect the wallet with both the Issuer and the Verifier when issuing credentials and when presenting them.

OpenID Connect Credential Provider: OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables relying parties to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User. In this project we extend the role of an OpenID Provider from being the provider of simple identity assertions into being the provider of credentials, as defined at [Lo21]:

1. The Holder acting as an OpenID Client sends a Credential Request to the Credential Provider that is acting as an OpenID Provider (OP).
2. The Credential Provider authenticates the End-User and obtains authorization.
3. The Credential Provider responds with a Credential.

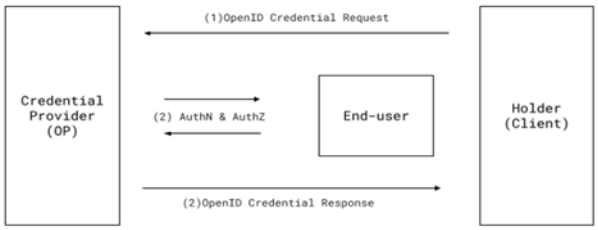

Figure 3: OpenID Connect Credential Provider

Self-Issued OpenID Provider – SIOP: OpenID Connect supports Self-Issued OpenID Providers (Self-Issued OPs, or SIOPs) [Op20]. These are personal OpenID Providers (OPs) that issue self-signed ID tokens, enabling portability of the identities among providers. We propose to use the wallet as a SIOP when interacting with the Issuer and

the Verifier during the authentication process and to provide the required EHIC credential.

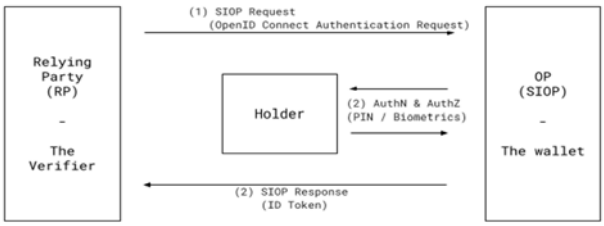

Figure 4: Self-Issued OpenID Provider - SIOP

4 SICPA bridge

Business problem: While the current state of the art in SSI is being driven by global open standards, this does not automatically guarantee practical interoperability between different implementations using a variety of protocols, credential types, and DID-methods. True interoperability is critical in preventing vendor and technology platform lock-in. This is of special importance to buyers that are essential in the market adoption of SSI systems. In addition, true interoperability is also key for adoption by holders, who i.e. should not have to worry about wallet management in order to facilitate different issuers or verifiers.

The consequences for businesses will be a higher cost structure to support different approaches (comparable to the iOS vs Android dilemma for developers) and to cope with a lack of flexibility and inability for systems to interoperate due to vendor lock-in. On the market side, application providers face a slow adoption rate and a limited subscriber base.

Solution approach SICPA bridge: The SICPA bridge enables trusted online peer-to-peer interactions based on interoperable distributed ledger technologies (DLTs), peer-to-peer (P2P) interactions across multiple did-methods, using standardized VCs. It provides a set of APIs to enable the usage of decentralized identifiers (DIDs), DID-communication, and VC exchange. From these building blocks, implementers can build issuance and verification services in a manner that is agnostic to any particular DID network, credential exchange protocol or credential type.

SICPA proposes the following technological building blocks for issuance and verification of VCs, that will enhance interoperability in the SSI ecosystem and lowers the barrier to adoption for all stakeholders in the market.

DIDComm and CHAPI protocol support: An Issuance and verification service that supports both DIDComm [De21], as well as the Credential Handler API (CHAPI) [Cr20b]. Supporting both protocols will increase the freedom of choice in wallets for the holder.

AnonCreds and [JSON-LD] credential type support: Integration of [JSON-LD] signing and verification in the Aries code-base [Hy19]. Providing both AnonCreds [LZ19]

and [JSON-LD] [JS20c] standards will greatly enhance the interoperability across the overall ecosystem and enable true portability of VCs

Support for multiple DID-methods: Native support for multiple issuers and verifier DID-methods in Aries. Offering multiple did-methods (e.g. did:sov, did:ala, did:eth) for issuers and verifiers will enable broad support across the ecosystem.

5 SSI-eIDAS bridge

The SSI-eIDAS bridge is a component that proposes to enhance the legal certainty of any class of VC, by incorporating the issuer's advanced or qualified electronic signature (if the issuer is a natural person) or seal (if the issuer is a legal person). Qualified certificates, defined under articles 28 (natural persons) and 38 (legal persons) of the eIDAS Regulation, can be used to confirm the identity of the natural or legal person. In the case of the electronic seal, Article 3 (29) of eIDAS Regulation defines the electronic seal certificate as "*an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person*".

Trustworthiness in a VC is linked to the issuer's DID: Verifying an issuer's identity is paramount, as there is no binding of a DID to a real-world natural or legal person per se.

The eIDAS regulation will evolve to be more technologically neutral and inclusive so that some of the benefits of using SSI can be achieved (fine-grained and specific attribute-based credentials, privacy improvements through selective disclosure, protocols for data sharing), but this will take time. The main role of the eIDAS Bridge is thus to assist (1) Issuers, in the process of signing/sealing a VC, and (2) Verifiers, in the last mile of the verification process, to help identifying the natural or legal person behind an issuer's DID.

5.1 Technical solution description

From a technical perspective, this electronic signature or seal is attached to the VC in form of a linked data signature, a special class of a linked data proof, according to [Li20a]. A linked data signature is a type of linked-data proof [LD-PROOF] consisting of information about the signature, parameters required to verify it, and the signature value itself. All of this information is provided using linked data vocabularies such as the security vocabulary [SECURITY-VOCABULARY], [Th21]. An example of the resulting proof follows, where a new proof type, 2020 CAdES RSA Signature Suite, has been defined:

```
"proof": {
  "type": "CAdESRSASignature2020",
  "proofPurpose": "assertionMethod",
  "created": "2019-08-23T20:21:34Z",
  "verificationMethod": "did:factom:5d0dd...3d99ef#MIIEE...suIcuV",
  "proofValue": "-----BEGIN PKCS7----- iG9wDQYLK... -----END PKCS7-----"
}
```

In any case, this linked data proof is verified using the issuer's qualified certificate; which must be resolvable and accessible to any relying party. To this end, different options are available. The certificate can be directly available in the `verificationMethod` of the proof structure or linked in the DID document of the issuer where it could be directly published or pointing to an online repository where the certificate could be published. Any person receiving a VC is able to lookup the DID, and then resolve the DID to get the DID Document; with the DID document, it is possible to access the qualified certificate contained in this repository, thus having access to the verified identity of the issuer.

5.2 eIDAS regulation discussion

As discussed in [Do20], "*the electronic seal must serve as proof that an electronic document has been issued by a legal entity, providing certainty about the origin and integrity of the document*", but it does not mean that it can be used by the legal entity for "*all legally binding actions, especially in accordance with the rules of representation of the different types of legal entities*". When using electronic seals to issue VCs it should be checked that its use does not conflict with national legislation. Regarding the use of qualified and non-qualified electronic seals, "*the eIDAS Regulation establishes a legal norm of non-discrimination of the electronic signature different from the qualified electronic signature, which also extends to the unqualified electronic seal*". This is shown in article 35 (1) of the eIDAS Regulation which indicates that "*an electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals*".

On the other hand, when a qualified seal is used, as per Article 35 (2) of the eIDAS Regulation, it "*shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked*", and also it benefits from cross-border recognition, per Article 35 (3), since "*a qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States*". The identification of the natural or legal person, which is the main purpose of digital certificates, is used to support the signature or advanced electronic seal by confirming the identity of the person concerned. The certificates are used thus to "authenticate" the identity of the natural or the legal person. Finally, it should be noted that in any case, the certificates must be issued by a Qualified Trust Service Provider, "*in compliance with the corresponding legal requirements applicable to an advanced or qualified electronic signature or seal*".

6 TRAIN

TRAIN is a lightweight trust management infrastructure for an open ecosystem of stakeholders and trust schemes. The train approach allows for the flexible definition,

consideration, publication of trust lists and verification of trust schemes compliance (e.g., eIDAS including LoAs or other Trust Schemes that can also be application/industry-specific) with different Levels of Assurances (LoA), using DNS as a root anchor. TRAIN aims to leverage this to support SSI infrastructures through a global trust infrastructure that can be used to verify the trustworthiness of issuers. The trust layer enables actors to verify the root of trust of certificates used to sign credentials. It is not dependent on a hierarchical CA infrastructure. The component builds on the infrastructure developed in the EU project LIGHTest (www.lightest.eu). Its trust layer is flexible: individual parties can define their own trust policies, manage, and publish them. TRAIN is fully in line with the open and decentral SSI approach and complements other approaches.

The trust management architecture that is made possible by TRAIN enables secure, trustable digital interactions. At the same time a classical hierarchical CA-type structure is avoided – so is fraud, chaos, and the pure dominance of the economically strongest actors in the system. Individuals or groups (industry organizations, NGOs, etc.) of verifiers can define for themselves the trust standards they require. Issuers can publish to what standards they comply. The system is open, but standards for trust are transparent, as the trust schemes and lists can be published. TRAIN adds a flexible trust layer to be used by verifiers to define their required level of trust. No central authority is established, everyone can issue certificates, but TRAIN facilitates individual trust decisions. Trust standards such as Trust Schemes (eIDAS, Pan Canadian Trust Framework, but also self-defined schemes and policies) can be integrated.

The two main components of the TRAIN infrastructure are briefly explained in the following.

6.1 Publication of trusted issuance services

The two types of publication authorities of the TRAIN Infrastructure are Trust Scheme Publication Authorities (TSPA) and Trust Publication Authorities (TPA). A TSPA is the higher-level component which is to develop and publish different trust schemes in the TRAIN infrastructure. A trust scheme comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust. For example: In the European Health Insurance Card use case, the European Commission is the TSPA and develops its own trust scheme.

A TPA in TRAIN is responsible for maintaining a list of trusted issuance services for credentials. Issuance services that meet the requirements of the trust scheme of the specific TSPA can be included in its trust list. Thus, it is transparent how issuance services get to be included in the trust list of a certain trust scheme. In our simple use case example, a TPA is operated by each individual national EU member country's government or National Health Insurance Provider (or another institution – depending on the national specifics). This TPA is then responsible for including the different insurance providers of the respective country in the trust list if they adhere to the guidelines of the trust scheme

issued by the European Commission. All the approved issuance service's DIDs will be published by the TPA on a trust list in the trust infrastructure. Since the TRAIN infrastructure uses the DNS as a root anchor, the hostname of the trust publication authority will have to be integrated in the credential in the form of a Domain Name. This is required to resolve the corresponding trust scheme from the credential. For example: When a national health insurance provider is the issuance service of the credential, and EHIC is the trust scheme publication authority, it will be published as EHIC.eu in the TRAIN Infrastructure.

Any trust scheme with any type of LoAs structure can be formalized and published through TRAIN. By adding an issuance service's DID to a trust list, the issuance service can be integrated into different trust schemes of TSPAs. The trust list is published under the corresponding trust scheme. For the use in an SSI infrastructure, the model of TS 119 612 – ETSI for trust lists was extended, so that the trust list can accommodate the DID of the issuance service which is used to resolve DID documents. It is important to note that multiple TSPAs/TPAs can be set up under the TRAIN infrastructure to scale globally and to cater different domains of trust. This gives verifiers the flexibility to subscribe to different trust lists and schemes based on different regions, preferences or use cases. Verifiers decide which TSPAs to use.

6.2 TRAIN infrastructure component for the verification service

The verification service of the verification application has an additional API to TRAIN to perform an external verification of the credential based on the hostname of the TPA and the DID URI of the issuance service using an API request. As a first verification step, TRAIN performs a DNSSEC request of the hostname to verify the chain of trust with the root DNS. Subsequently, a query is made using the hostname to locate the corresponding pointer mapped to trust scheme and trust list. Then, the pointer of the trust list is queried to fetch the details of the issuance service DID. The DID obtained from the trust list is used to verify the issuer service DID from the credential. By doing so, the inclusion of this specific issuance service in the trust list of the specific TPA can be verified and the verification service will receive the verification results. Various trust schemes with different LoAs can be queried based on the respective requirements.

7 Conclusion

Decentralized identity uses cryptography to allow individuals to create and control their own unique identifiers. They can use these identifiers to obtain VCs from different stakeholders and prove the integrity and authenticity of these credentials to relying parties. However, for use-cases where individuals share their information across trust domain boundaries, providers should have in place the needed practices, policies, and other controls that apply regardless of such differences. With our concept, we have

demonstrated technical interoperability of the issuance, presentation, and verification of VCs incorporating different levels of assurance and trust domains in an eIDAS compliant way. Furthermore, the European Health Insurance Card (EHIC) is presented as an example to illustrate how, by providing a common framework, different participants in an ecosystem can increase trust. The presented concept builds bridges between Decentralized identity and trust / legal frameworks, showing how decentralized identifiers and VCs could be used as a base to provide trust to electronic services in a cross-domain ecosystem.

Some open issues and areas for future work remain. As of now, the initial enrolment of the issuer via publication of the issuer DID in the trust publication authority (TPA) is a manual process. As an improvement, this governance process could be supported through an API to enable some form of automation. Moreover, the creation of verifier policies is currently a manual process that doesn't provide a good user experience - particularly for verifiers without programming knowledge. Hence, a user-friendly verifier policy management tool with a graphical user interface building on work in LIGHTest [WO21] and/or in ESSIF-Lab [PO21] should be integrated into the concept.

As mentioned in this paper, the trust publication authority's hostname is included as a claim in the credential in the form of a Domain Name. This step is needed since TRAIN uses the Domain Name System (DNS) as a root anchor, and as an issuer, their DID can be published in multiple trust publication authorities (TPA).

We acknowledge that further exploration is needed to improve the proposed solution. One line of work could be to publish DIDs in the DNS for discovery on an hostname's base, as discussed in [MKS20]. A verifier based on their verification policies could determine if the given issuer belongs to one of the Trusted List of the trust publication authorities configure in the verification policies. By doing so, not only we will avoid the inclusion of the extra claim in the credential, but it would allow us to define the identifier of the issuer as a URI instated of only a DID, as specify in the VC data model. As of per today, there are no eIDAS Qualified Trust Service Providers that provide SSI-eIDAS Bridge services. Someone implementing a qualified SSI-eIDAS Bridge service would need to integrate a remote qualified e-sealing service to benefit from cross-border recognition and presumption of correctness of the origin of that data as stated in Article 35 (2) of the eIDAS. Finally, due to the constraints of the format of the conference, our presentation focusses on a technical approach to trust in SSI. It is important to highlight that this needs to be complemented by legal and regulatory development efforts, such as [Do20].

Bibliography

[Cr20] W3C: Credential Handler API 1.0. w3c-ccg.github.io/credential-handler. accessed: 01/03/2021.

[De21] Decentralized Identity Foundation: DIDComm Messaging Specification. identity.foundation/didcomm-messaging/spec/. accessed: 01/03/2021.

[Do20] Domingo, I.: SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market, 2020.

[ES21] ESSIF-LAB | ESSIF-LAB: Help Shape a Safe and Secure Next Generation InternetT GENERATION INTERNET. essif-lab.eu/. - accessed: 01/03/2021.

[Eu14] European Parliament: Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union (Regulation Nr. 910/2014). Brussels, Belgium: European Parliament, 2014.

[Eu21] European Commission: European Health Insurance Card. ec.europa.eu/social/main.jsp?catId=559&langId=en. accessed: 01/03/2021.

[Hy19] Hyperledger/aries-rfcs. github.com/hyperledger/aries-rfcs. accessed: 01/03/2021.

[JS20] W3C: JSON-LD 1.1. w3.org/TR/json-ld11/. accessed: 01/03/2021.

[Li20] W3C: Linked Data Proofs 1.0. w3c-ccg.github.io/ld-proofs/#linked-data-signatures. accessed: 01/03/2021.

[Lo21] Looker, T. et.al.: OpenID Connect Credential Provider. mattrglobal.github.io/oidc-client-bound-assertions-spec/. accessed: 01/03/2021.

[LZ19] Lodder, M.; Zundel, B.: Anonymous Credential Protocol - Hyperledger Indy HIPE documentation. hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0109-anoncreds-protocol/README.html. accessed: 01/03/2021.

[MKS20] Mayrhofer, A.; Klesev, D.; Sabadello, M.: The Decentralized Identifier (DID) in the DNS. datatracker.ietf.org/doc/draft-mayrhofer-did-dns/?include_text=1, accessed: 01/03/2021.

[MM21] Marangoni, M.; Martinez Jurado, V.: European Health Insurance Card v0.1. essif-lab.pages.grnet.gr/interoperability/eidas-generic-use-case/. accessed: 2021-03-01.

[Op20] OpenID Foundation: openid / connect / openid-connect-self-issued-v2-1_0.md — Bitbucket. bitbucket.org/openid/connect/src/master/openid-connect-self-issued-v2-1_0.md. accessed: 01/03/2021.

[PO21] Policyman Project: ESSIF-Lab/business/PolicyMan_project_summary. gitlab.grnet.gr/essif-lab/business/policyman/policyman_project_summary. accessed: 01/03/2021.

[Th21] W3C: The Security Vocabulary. w3c-ccg.github.io/security-vocab/. accessed: 01/03/2021.

[VR20] W3C: Verifiable Credentials Data Model 1.0. w3.org/TR/vc-data-model/. accessed: 06/02/2020.

[WO21] Weinhardt, S.; Omolola, O.: Usability of Policy Authoring Tools: A Layered Approach. In: 2021 — ISBN 978-989-758-359-9, pp. 301–308, 2021.