DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust

Clemens Brunner
Center for Secure Energy Informatics
Salzburg University of Applied Sciences
Austria
clemens.brunner@en-trust.at

Ulrich Gallersdörfer
Software Engineering for Business Information Systems
TU Munich
Germany
ulrich.gallersdoerfer@tum.de

Fabian Knirsch
Center for Secure Energy Informatics
Salzburg University of Applied Sciences
Austria
fabian.knirsch@en-trust.at

Dominik Engel
Center for Secure Energy Informatics
Salzburg University of Applied Sciences
Austria
dominik.engel@en-trust.at

Florian Matthes
Software Engineering for Business Information Systems
TU Munich
Germany
matthes@tum.de

ABSTRACT

Decentralized identifiers and verifiable credentials have been proposed as a self-sovereign and privacy-friendly alternative to centralized and proprietary authentication services. Currently, a W3C standard exists that attempts to unify existing proposals and to find a common layer for decentralized identification and verification. However, there are some limitations of decentralized identifiers in comparison to established, centrally controlled authentication platforms concerning trust, privacy and usability. In this paper, we first describe all workflows which are necessary to create, share and verify a verifiable credential and second, we discuss the limitations concerning trust, privacy and usability of decentralized identifiers. The paper summarizes the involved workflows for decentralized authentication as proposed by the current standard. Further, we show the existing limitations and shortcomings that need to be considered when sharing DID for practical implementations and give an overview of possible solutions and future directions.

CCS CONCEPTS

• **Security and privacy → Authorization**; **Privacy-preserving protocols**; **Digital signatures**; • **Computer systems organization →** Distributed architectures;

KEYWORDS

Decentralized Identifiers, DID, Verifiable Credentials, VC, Verifiable Claims, Blockchain, Trust, W3C, Web of Trust

Preprint, December 2020, Online

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Clemens Brunner, Ulrich Gallersdörfer, Fabian Knirsch, Dominik Engel, and Florian Matthes. 2020. DID and VC:, Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In *Proceedings of Preprint*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Authentication and verification has become one of the major present challenges in the world wide web. This is not limited to individuals, but also applies to institutions and to devices in the context of the Internet of Things. Dominated by centralized authorities and proprietary services, the field of authentication has become much more centralized and less self-governed than originally designed and desired. With the advent of blockchain technology and distributed ledger, a novel, fully decentralized and permission-less approach has been established, that seems promising for self-governance and self-sovereignty. Recently, decentralized identifiers (DIDs) and verifiable credentials (VCs) have been proposed as a modern, decentralized and lightweight alternative to established authentication methods [13, 17]. DIDs build to a large extent on the foundations laid by distributed ledger technology and use them as a major building block. Complemented by VCs, this allows for a purely non-tangible and digital authentication with services and applications. A DID acts as an unique identifier and refers to a DID document, which contains the information about an identity. VCs are then used to store and represent machine-readable credentials.

There are, however, some limitations and DIDs and VCs alone are not sufficient for undoubtedly proving an identity. Furthermore, the interoperability between the currently evolving DID methods is limited and usability issues (such as storing and managing cryptographic key material) are evident. In this paper, we describe the workflow for decentralized identities and discuss the practicability of the proposed standards [13, 17]. The contribution of this paper is twofold: First, the roles of the issuer, of the receiver and of the verifier within the context of DIDs and VCs are described and the

full workflow from the creation of a DID to the verification of a claim is outlined. This is done in adherence to the standard. Second, we discuss the limitations of decentralized identities and analyze the underlying trust assumptions. The outcome of this paper serves as both, a guideline for others, planning to use DIDs and VCs, and as a basis for implementing DIDs and VCs in existing or novel use cases.

The rest of the paper is structured as follows: Section 2 provides information about DIDs, VCs and Self-Sovereign Identities (SSI). Section 3 describes a workflow in detail. Section 4 discusses limitations and open issues with DIDs and VCs. Section 5 provides an overview of three major contributors to the SSI ecosystem and Section 6 summarizes this paper and gives an outlook to future work.

2 BACKGROUND

This section introduces the relevant background for the description of the workflow and for the discussion of open issues with DIDs and VCs.

2.1 Self-sovereign Identity

An SSI is a concept of identity, where the individual is free to claim its own identity without a centralized trusted party [14]. Other than with centralized or federated identities, there is no single trusted party or a defined subset of trusted parties that act as such a root [1]. The concept has grown with the emergence of blockchain technology, which provides the necessary ecosystem for establishing a fully decentralized and SSI. According to [1], the key properties of such an identity concept can be summarized as follows: (i) the claim of an identity is independent of other instances and claims, under full control of the owner, including access to all relevant data, and generally long-living; (ii) the systems and algorithms are open and thus ensure full portability and interoperability among parties; (iii) the release of any data must be under the consent of the owner, kept at a minimum and the rights of the owner must be protected at any time. This, in summary, defines the framework for DIDs, which is attempted to be implemented in, e.g., the W3C standard of DIDs [14].

2.2 Roles

The roles relevant for DIDs and as described by this standard [14] are *Subject*, *Receiver* and *Relying Party*. Note that this paper uses – in parts – different terms in adherence to common cryptographic notation. The Subject is denotes as *Issuer* and the Relying Party is denoted as *Verifier*.

2.3 Decentralized Identifier

A DID is a globally unique reference linking to a DID document and is in the form `did:<DID method>:<method-specific identifier>` [14]. The DID method is a reference to a specific distributed ledger or network and the method-specific identifier allows to resolve the DID within that reference. Given a DID, one can retrieve the referenced DID Document, such as one would do with an URL to locate, e.g., a web resource.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "id": "http://example.edu/credentials/42",
  "type": ["VerifiableCredential"],
  "issuer": "did:example:deeb1f712ebcc276e12ec42",
  "issuanceDate": "2020-06-10T04:20:00Z",
  "expirationDate": "2020-10-10T04:20:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebcc276e12ec21",
    "name": "John Doe"
  },
  "proof": {
    ...
 }
}
```

Figure 1: Example of a Verifiable Credential

2.4 DID Method and DID Document

A DID Method is a specific description of how a DID is resolved in a particular blockchain or distributed ledger and how DID Documents are written and updated. A DID Document is a structure expressed in, e.g., JSON and contains information about the identity, such as public keys. A DID Document also includes references to service endpoints, where the issuer can operate certain services, such as a repository for VCs. An example for a distributed ledger, including a specified DID Method where one can store DID Document for establishing and maintaining a SSI is Sovrin [16].

2.5 Verifiable Credentials, Claims and Presentations

A VC is a form of machine-readable credential that is, according to the specification in [17], cryptographically secure and privacy-respecting. A VC is bound to a DID in a DID Document and thus linked to an identity. In Figure 1 an example VC containing a name as attribute is illustrated.

A VC is created by the issuer and sent to the receiver. It contains a set of claims about attributes, e.g., name, birth date, grade, ID, or other information the issuer wants to attribute to the receiver. In order to forward a claim to a verifier, a presentation is created. A presentation allows to present only a subset of attributes, such as revealing the birth date attribute without the name attribute.

3 WORKFLOWS

In this section the workflows starting with the creation of a DID and ending with the verification of a claim generated out of a VC are presented in accordance with the standard [14]. The workflows are separated by the involved actors: the issuer (I) of a VC; the receiver (R) of a VC and the verifier (V) of selected claims. The overall workflow is depicted in Figure 2. We discuss limitations and shortcomings in the following Section 4.

3.1 Issuer

In this section, the workflow for the issuance of a VC from an I to a R is described.

- **Creating a DID for I:** The first step to issue a VC is the creation of the DID. I can select a DID method. A list of

available DID methods can be found in [18]. Additionally, I can choose if it wants to create a new DID for each VC or using the same DID for all VC. However, in case that I should be publicly verifiable, e.g., in the case when I is represented by a university, there will be no need for creating multiple DIDs.

- **[Optionally] Updating DID document:** The *DID's* corresponding cryptographic keys are described in a DID document, which can be resolved by only knowing the DID. I can have multiple DID documents where, e.g., key update operations are described. Note, that the owner of a DID is responsible for the backup of the private keys. In case that I loses the private key, there is no default way to recover it [3].
- **Collection and verification of R:** Once the DID and the corresponding DID documents are created, I needs to know R's DID before the VC can be generated. For this, I needs to provide a way to collect and – if needed – verify the identity of R. It depends on the type of the VC if an identity check is needed, e.g., a VC representing an attendance confirmation requires a weaker identity check than a VC representing a passport or driver license.
- **Issuing VC to a R:** After I created a DID and collected the DID of R, I is able to create a new VC. The VC includes at least the DID of I and R and is digitally signed with I's DID. After the VC is created, I will send it to R.
- **[Optionally] Revoking a VC:** After handing the VC to R, I has no way to delete the issued VC anymore. However, some DID methods describe a way to revoke already issued VCs, Sovrin, for instance, uses cryptographic accumulators [16] for the revocation.

3.2 Receiver

In this section the workflow for the receiver (R) of a VC is described.

- **Creating a DID for R:** R needs to create a DID before it is able to receive VCs. The process is similar to the creation of a DID for V, the verifier. R may create a new DID for each VCs. This will preserve the privacy of R, because it makes it harder for V, or another verifier, to link different VCs which are issued to the same receiver R.
  R is fully responsible for the backup of its own private keys. In contrast to I, which could be represented by an organisation, e.g., a university or a government, where IT experts are employed, R is represented by an individual person, who may have no prior knowledge about managing cryptographic keys.
- **Sharing DID with I:** To receive a VC R needs to share the DID with an issuer I. It depends on I, how this operation works and if additional identification mechanism is required.
- **Receiving VC from I:** After successfully setting up a DID and sharing it with an issuer I, I will create the VC and transmit it to R. Once this process is done, R is able to share selected claims contained in a VC with anyone.
- **Creating VP out of VCs for a V:** A VC contains one or more claims, e.g., name, date of birth, type or further information about R. In order to preserve privacy, R is able to select a subset of claims attached to a VC and create a VP of those selected attributes. The VP contains only the needed information, and not more than the R is willing to share.
- **Sharing a VP with a V:** The created VP can be shared with a V. There is no standard procedure how this process is done, it depends on the communication methods used by R and V.

3.3 Verifier

In this section the workflow for V of a VC is described.

- **Receiving a VP:** In contrast to I and R, V does not need to create a DID before verifying a VP. To verify a VP, V first needs to receive it. The transmission of the VP depends on the communication methods[1] of R and V.
- **Resolving DID Documents from I and R:** A VP contains of one or more Cs about R. The following verification steps must be done for each claim: To verify a claim, the first step is to collect the DID documents of R and I. The process to resolve a DID document out of a DID is described in the specification of the DID method.
- **Verifying signatures of R and I:** With the keys attached to the resolved DID documents V can verify, if the signatures of the are generated by I and R.
- **Checking revocation information:** If the DID methods allow for revocation of VC, V needs to check if the VC is still valid and not revoked. This process must be described by the DID method specification.
- **Verifying Identities for R and I:** The last step to check if a is valid is to verify the identities of R and I. This process is not described in the DID W3C standard [14]. At the time of writing, there is no automated workflow proposed in the standard for identification of the identities behind a DID.

4 DISCUSSION

This section discusses issues related to DIDs and VCs, such as trust assumptions and privacy, as well as challenges related to revocation and usability aspects. These issues are at the time of writing not sufficiently addressed within the standard.

4.1 Trust

DIDs aim to shift authentication away from a centralized authentication provider (e.g. centralized approaches or federated such as OAuth[9]) to a decentralized infrastructure. While this is a promising attempt and can be used in pseudonymous environments (e.g., public bulletin-boards), there are specific yet unsolved challenges this ecosystem faces. The latter is especially evident in the context of legal interaction and transactions.

The cryptographic premises are well suited to prove and verify the possession of a DID, however, there is no integrated means of connecting the real-world identity to the DID's owner. While we are able to attach VCs to DIDs and therefore would be able to endorse personal information (e.g., name, date of birth,...) to a DID, the standard does not describe how the trust in the I can be established.

[1] This includes email transfer, download, personal exchange, etc.

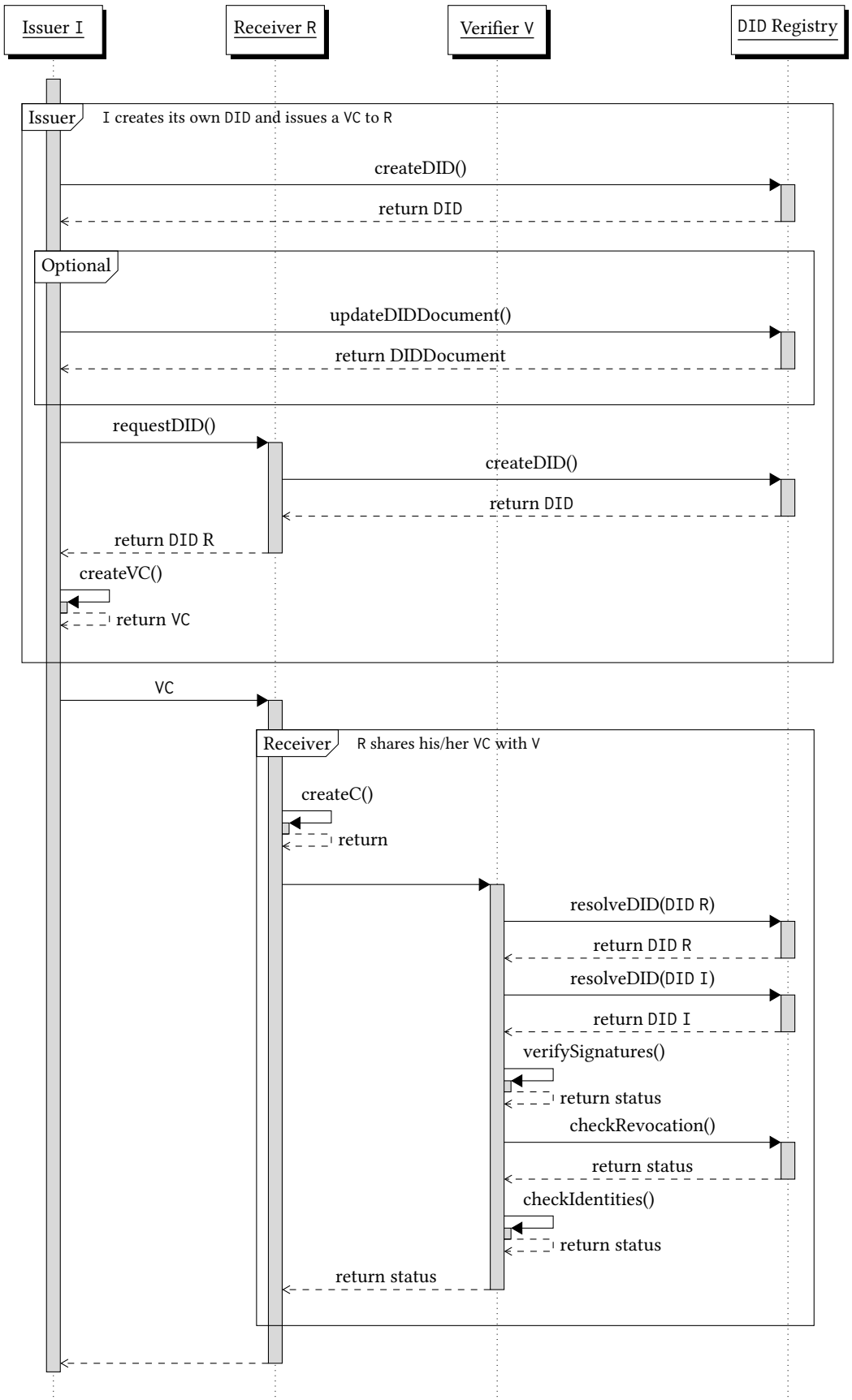

Figure 2: Issuance, Sharing, and Verification of a Verifiable Credential

In traditional digital systems, e.g., the World Wide Web, this is usually facilitated by a root of trust or multiple roots of trust, e.g., Certificate Authorities (CA). CAs are certified companies; their business model relies on providing verified and up-to-date information about the binding of the real identity and the digital identity of individuals, institutions and other entities.

From our perspective, there are two potential solutions:

- A promising approach is the establishment of a Web of Trust of public issuers. This has been applied to other domains, such as identities for email communication as PGP [22]. This would enable that trustworthy institutions vouch for entities they have knowledge of and allow these entities to display their credentials to other parties, ensuring a connection to a real-world identity, e.g., [4].
- Alternatively, a hybrid approach could be implemented by the integration of CAs [5] into the DID ecosystem [8]. This combines the decentralized authentication infrastructure with established roots of trust.

4.2 Privacy

It is often claimed that DIDs and VCs lead to the ability to "own" and "control" one's data[2]. While, this is a promising claim, but infeasible in practise.

If pseudonymous information is used for authentication, DIDs do not provide any advantages in comparison to traditional approaches (e.g., pseudonymous email address), as the data provided itself does not make a statement about the real world identity of the user. Once, personal data linked to an individual, e.g., name, date of birth, credit card,..., has been shared, this information is in possession of R and can be used for further means (e.g., advertisements). The owner of the data has no option to force the deletion, apart from legal claims [10].

Claims of personal data, e.g., a proof that a person is older than 18 years, can be shared in a way using zero knowledge proofs, without disclosing the date of birth itself. However, this applies only to specific claims about the existence and ranges of attributes.

4.3 Revocation

In principle, two potential reasons exist for revoking a credential or a DID:

- The key material expires, got lost or stolen
- The real-world status about the VC has changed, e.g. a degree was obtained maliciously and has to be revoked.

The revocation of DIDs and VCs is part of the standard. However, the DID specification does not make a statement about the timestamp of the revocation and creation of DIDs and VCs. Tamper-proof timestamping (as available in many blockchain networks) allows to prove that a DID or VC was valid for a certain period of time. For example, if a university issued multiple VCs over a period of time and has to revoke its own DID because of compromised key material, the issued VCs remain valid (if not revoked otherwise). An attacker would not be able to further issue valid credentials, as they have been issued after the key material was revoked. Timestamping VCs on a blockchain network would enable this feature.

4.4 Usability

The DID ecosystem is based on public key infrastructures where the users are in full control of their cryptographic material, e.g., the private key. This is similar to blockchain-based systems, in which the users control the access to their assets [3]. This leads to following issues regarding usability:

- Recovering a lost private key is not possible
- Form of authentication is solely based on information, attacks may lead to significant data and identity loss
- Remembering private keys is not possible due to their length and randomness

Overall, all users are fully responsible for creating and managing a secure backup of their private keys. This might lead to a reduced adoption of end users. Approaches like the Universal Authentication Framework [11] and respective hardware might enhance the user experience and managing their cryptographic key material.

5 RELATED WORK

SSI, DIDs, and VCs so far have attracted little attention in the academic discourse[12].

To account for the lack of scientific publications, we identify three major forces for contributions towards the advancements of SSI and DIDs:

- The community *Rebooting Web of Trust*,
- the W3C groups evolving around DIDs and VCs, and
- private companies pursuing the usage of these technologies.

In this section, we outline the work of these three forces and further elaborate on the current scientific situation.

5.1 Rebooting Web of Trust

Rebooting Web of Trust is a community that focuses on advancements in DIDs and VCs and is led by Christopher Allen and Joe Andrieu[19]. Christopher Allen also outlined the vision for SSI in 2016 [1]. The group regularly conducts workshops and publishes the results of this work on Github[20, 21]. They deal with a variety of issues within the SSI ecosystem[6], propose enhancements to existing blockchain applications to adhere to DIDs and VCs [15] or discuss reputation of actors inside trust networks[2]. By this, they contribute to the current discussion and demonstrate enhancements and further developments for SSI.

5.2 World Wide Web Consortium

The *World Wide Web Consortium* (W3C) is the entity for standardizing technologies in the World Wide Web. Its responsibility is to oversee the work on DIDs Data Model [13] and VCs Datamodel [17]. The work on these proposals is conducted by so-called W3C working groups, which discuss their thoughts and comments on Github[3] and in public mailing lists[4]. The main outcome of these

[2]E.g., Microsoft "believes" everyone has the right to own their digital identity, one that securely and privately stores all personal data" https://www.microsoft.com/en-us/security/business/identity/own-your-identity Last Access [June 2020]

[3]Discussions on Github can be found at https://github.com/w3c/did-core/ and https://github.com/w3c/vc-data-model/

[4]https://lists.w3.org/Archives/Public/public-vc-wg/

groups are the standards (or proposals themselves) as their additional published information is sparse. For example, alongside the DID spec, they have an updated list about current DID methods[18].

5.3 Private Companies

Private companies like Evernym or Sovrin also publish a variety of opinion papers and technical specifications [7]. As they are private companies, they are interested in turning these technologies into profit by consulting other firms or institutions to adopt to the technologies of DID and VCs. However, some of the employees of these companies are also part of the WoT and W3C and influence the decisions made within these communities. From outside, it remains unclear if these companies always act in the best interest of the community when shaping the standards of DIDs and VCs.

6 CONCLUSION

In this paper, we outlined the characteristics of decentralized identifiers, verifiable credentials and self-sovereign identity in general. After introducing terms and relationships between the terms, we outlined an exemplary workflow which discusses the steps necessary by each party to conduct the issuance, sharing and verification of a verifiable credential. Further, we discussed the difficulties and potential issues of these concepts, which could hinder further adoption or lead to unnecessary barriers in bootstrapping. We here show, that these concepts are currently promising, but demonstrate points for further enhancement in these systems.

ACKNOWLEDGEMENTS

The financial support by the Federal State of Salzburg is gratefully acknowledged.

REFERENCES

[1] Christopher Allen. 2016. The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[2] Arthur Brock, Kaliya Hamlin, Grace Rachmany, and Jakub Lanc. 2019. Reputation Interpretation. https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/reputation-interpretation.pdf
[3] Clemens Brunner, Günther Eibl, Peter Fröhlich, Andreas Sackl, and Dominik Engel. 2020. Who stores the private key? An Exploratory Study about User Preferences of Key Management for Blockchain-based Applications. submitted to ICISSP 2021.
[4] Clemens Brunner, Fabian Knirsch, and Dominik Engel. 2019. SPROOF: A platform for issuing and verifying documents in a public blockchain. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. SciTePress, Prague, Czech Republic, 15–25.
[5] Council of the European Union. 2014. 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. *Official Journal of the European Union* 57, L 257 (2014), 73–114. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910
[6] P. Dingle, S. Hammann, D. Hardman, C. Winczewski, and S. Smith. 2020. Alice Atempts to Abuse a Verifable Credental. https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/alice-attempts-abuse-verifiable-credential.pdf
[7] Evernym. 2020. White Papers. https://www.evernym.com/white-papers/
[8] Ulrich Gallersdörfer and Florian Matthes. 2020. AuthSC: Mind the Gap between Web and Smart Contracts. arXiv:cs.CR/2004.14033
[9] Dick Hardt et al. 2012. *The OAuth 2.0 authorization framework*. Technical Report. RFC 6749, October.
[10] Galia Kondova and Jörn Erbguth. 2020. Self-sovereign identity on public blockchains and the GDPR. In *35th Annual ACM Symposium on Applied Computing*. ACM, Brno, Czech Republic, 342–345. https://doi.org/10.1145/3341105.3374066
[11] Rolf Lindemann, Davit Baghdasaryan, and Eric Tiffany. 2014. FIDO Universal Authentication Framework Protocol. *Version v1. 0-rd-20140209, FIDO Alliance, February* (2014).
[12] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A survey on essential components of a self-sovereign identity. , 80–86 pages. https://doi.org/10.1016/j.cosrev.2018.10.002
[13] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2019. Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/
[14] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2020. Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. DIDs v1.0. https://www.w3.org/TR/did-core/
[15] Anthony Ronning and Wong Wai Chung. 2019. Blockcerts V3 Proposal. https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/final-documents/BlockcertsV3.pdf
[16] Sovrin Foundation. 2018. *Sovrin: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust*. Technical Report January. https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf
[17] Manu Sporny, Dave Longley, and David Chadwick. 2019. *Verifiable Credentials Data Model 1.0*. Technical Report. W3C. 1–115 pages. https://w3c.github.io/vc-data-model/https://www.w3.org/TR/vc-data-model/
[18] Orie Steele and Manu Sporny. 2020. DID Method Registry. https://w3c-ccg.github.io/did-method-registry/#the-registry
[19] WebOfTrustInfo. 2018. Rebooting the Web-Of-Trust. https://www.weboftrust.info/
[20] WebOfTrustInfo. 2020. Rebooting Web of Trust: White Papers. https://www.weboftrust.info/papers.html
[21] WebOfTrustInfo. 2020. WebOfTrustInfo/rwot10-buenosaires: CANCELLED: RWOT10 in Buenos Aires, Argentina (March 2020). https://github.com/WebOfTrustInfo/rwot10-buenosaires
[22] Duane Wilson and Giuseppe Ateniese. 2015. From pretty good to great: Enhancing PGP using bitcoin and the blockchain. In *International Conference on Network and System Security*. Springer, 368–375.