CHAPTER 5. WEB TECHNOLOGIES FOR DECENTRALISED IDENTITY[1]

Víctor Rodríguez Doncel[2]

Abstract. This chapter analyses technologies that support decentralised identity on the Web. The World Wide Web Consortium, which maintains the technical specifications of the Web, has consistently advocated for decentralised models for sharing information. Some of their latest recommendations include the specification of a Decentralised Identifier (DID) and a Verifiable Credential (VC) following the Semantic Web principles. The claims contained in these credentials can be algorithmically verified without the intervention of authorities. These technologies are often associated with implementing the Self-Sovereign Identity paradigm, and this chapter evaluates whether this will happen in practice, particularly in the context of the financial sector. Whereas some privacy concerns are identified, the integrated use of DID, VC and Open Digital Rights Language ODRL will present clear benefits in at least some commercial settings.

Keywords: World Wide Web Consortium, Self-Sovereign Identity, Decentralised Identifiers, Verifiable Credentials, ODRL

5.1. INTRODUCTION

Having an identity is essential for being allowed to do things. For example, attending an exclusive party is possible by holding a physical invitation card, which identifies the holder as one of the invitees. Moreover, identifying others is useful for exerting control over them. Simply put, and to use an analogy, the goatherder must identify each goat with a proper name to avoid losing them. The legal recognition of a person also captures these two opposite dimensions of empowerment and control: we have rights and obligations before the law. Being recognised before the law is a very strong right: "Everyone has the right to recognition everywhere as a person before the law", —reads Article 6 of the Universal Declaration of Human Rights. And this recognition also very strongly obliges us to pay taxes. So, we are goats that can go to parties.

The novelty in the digital world is that there are so many parties. As our lives happen more and more in the digital sphere, we consume more and more online services for any practical aspect of life. Sometimes, in exchange for our money, more often in exchange for our attention (we are obliged to watch ads) or in exchange for our data (involving more or less dubious practices about our privacy). In any case, we have a *user account* in a myriad of internet services —although perhaps we should express it conversely: the service provider has an account with our money committed, our time employed, and our preferences and habits revealed. In this scenario, we have multiple digital *identities*.

By choice or by force, we disclose different aspects of our lives to these service providers. And very easily, we forget what we said to whom –we are content if we can remember the many usernames and passwords we must use daily. We may have some rights as per regulation. In Europe, the General Data Protection Regulation protects citizens' privacy. Still, in practice, there are so many data controllers and privacy policies we have not read that we cannot control the data controllers. There is a technical shortcut if we identify ourselves in this plethora of systems through large identity providers, such as Facebook Connect or Google Sign-in. Most surely, we have all seen these buttons inviting us to "Log in with Google". But then, by doing so, we are further empowering these giants who already know so much about us.

---

[1] This paper expands and updates the text of the lecture delivered at the III International Congress entitled “Present and future of crypto-assets regulation in the European Union", held at the University of Alicante (Spain) on 13,14, and 15 December, 2023. This work is funded within the framework of: Proyecto CIPROM/2022/26 “Presente y futuro de la regulación de los Criptoactivos en la UE [Legalcripto]”. Proyecto Prometeo CIPROM/2022/26, grupos de investigación de excelencia, de la Generalitat Valenciana (P.I. Carmen Pastor). This work has also been supported by the Ministerio de Transformación Digital y Función Pública under the project "Infraestructura para la Investigación de Espacios de Datos distribuidos en UPM" (INESData)

[2] Associate Professor. Departamento de Inteligencia Artificial, Universidad Politécnica de Madrid (Spain). vrodriguez@fi.upm.es I do prefer my email not to be published.

The main problems to be solved in any identity system are avoiding the repetition of identifiers and authenticating the identified entities, e.g., proving you are the one you claim to be. The easiest way to solve these problems is to keep a centralised record of identities (for example, my list of goats or the centralised database of the tax-payers national IDs). However, there is an emerging alternative to this paradigm. This alternative is the idea of *decentralised identity*, a method of identifying and authenticating users or entities online without the need for a centralised authority. The concept of "Self-Sovereign Identity", often referred to by its acronym SSI, is a refinement of the decentralised identity idea that emerged in 2016[3][4]. In a self-sovereign identity system, individuals *own* and *control* their identity without the intervention of administrative or commercial authorities. Under SSI, a person's identity "is neither dependent on nor subjected to any other power or state"[5].

SSI restores in the digital world the same freedom and capacity for trust people had in the physical world before digital services arrived. Decentralised identity systems enable decentralised Personal Information Management Systems (PIMS), systems designed so that individuals regain control of their personal data—see the work of Zichichi et al. on how decentralised systems can be used to build such a PIMS[6].

SSI is still very young, and there is no prevailing technological implementation of the idea; different competing initiatives have been proposed. This chapter will only pay attention to one of the solutions based on Web standards. The reason for this choice is threefold: first, historically, the Web community has strived for distributed systems since the very beginning; second, this technology has received official support from different authorities; and third, solid implementations exist.

The chapter introduces in Section 2 the World Wide Web Consortium as the organisation standardising the Decentralised Identifier and the Verifiable Credential —these are described in Sections 3 and 4, respectively. Section 5 describes the ODRL policy language and proposes its joint use with the credentials. Section 6 analyses the use of these technologies in Fintech and their real value as implementations of SSI and electronic commerce.

5.2. THE WORLD WIDE WEB

Everybody knows what the World Wide Web is: a collection of computer files hosted on distant computers that are globally accessible. These files can be retrieved across different information systems because, relying on heterogeneous data transmission technologies, computers ultimately implement a series of standards and protocols that make the transfer possible. To read more about the importance of technical interoperability.

The famous TCP and IP are low-level protocols capable of reliably transporting data between two internet nodes, and they have been adopted as international standards by the Internet Engineering Task Force (IETF). The Internet infrastructure is the base for many other upper-level protocols and services, including Web protocols. Protocols such as HTTP or HTTPS transport documents of any kind on the Web, including hypertext documents (HTML). HTML, CSS and XML are some of the technical specifications maintained by the World Wide Web Consortium (W3C).

The W3C was founded in 1994 by Tim Berners-Lee with the mission "to lead its full potential by developing protocols and guidelines that ensure the long-term growth of the Web". The W3C organisation has an open nature itself: companies, public institutions and individuals work together to draft the technical specifications. Although the W3C has conflict resolution mechanisms, voting is rarely necessary, for consensus is sought as a rule. Discussions occur transparently, and anyone can implement the resulting norms, for they must be patent-free and royalties-free. Unlike the norms from other standardisation bodies, such as ISO/IEC, W3C's recommendations are always freely accessible. New specifications are dynamically created (or abandoned) to respond to the web users' and industry's needs, and the consortium merely plays a coordinating role with a very light bureaucracy. Therefore, it is fair to say that the

[3] Tobin A (2016)
[4] Allen C (2016)
[5] Preukschat A (2021)
[6] Zichichi M (2022)

decentralised information system *par excellence*, the World Wide Web, is technically specified in a rather decentralised way.

Many say that the Internet was decentralised by design to be resilient and withstand the technical failures expected in global warfare scenarios. The Web was decentralised by design to spread worldwide the ability to publish and obtain instant, connected information and knowledge[7]. The importance of the Web's paradigm shift cannot be overstated. Never in human history has the ability to obtain and publish information been so universally accessible. The revolution is not just about the vast amount of information available virtually everywhere, at any time, and for anyone. It is also about the diversity of sources providing this information. Despite the re-centralisation forces at play, the web is essentially decentralised with search engines, social networks, generative AI system providers, and other walled-off information sources.

On the World Wide Web, humans and machines have always had equal access to published pages, with computer programs retrieving information automatically just as humans do. Over time, the W3C's most significant endeavour became the further development of this concept. Tim Berners-Lee named this idea the *Semantic Web*:

> I have a dream for the Web [in which computers] become capable of analysing all the data on the Web – the content, links, and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled *by machines talking to machines.*[8]

The Semantic Web transformed a network of documents accessible by humans into a network of documents and data, where machines will consume data[9], many of them IoT devices. These humans and machines indistinctively exchange information in a non-hierarchically organised structure. Many have described this decentralised organisation as *rhizomatic*, in Deleuze and Guattari's sense[10]Rhizome is a term used in botany to describe a type of plant stem that grows horizontally underground. Unlike hierarchical root systems, rhizomes form a network of interconnected roots and shoots, embodying a non-hierarchical, decentralised structure. Deleuze and Guattari did not know the Web when they described this possible arrangement of information and knowledge, but the network structure of the Web certainly follows the pattern. Will identity systems adopt this form someday?

The early Web architects strived for simplicity, openness, and decentralisation. However, the initial design lacked a system to verify the identity of users or machines connecting to it —an identity layer of technologies. This identity layer was not a priority at first, and only with the growth of online services did new identity management systems and protocols become integral to the modern web. Kim Cameron, who was Microsoft's Chief Identity Architect for many years, put this bluntly: "The Internet was built without an identity layer." He meant that there existed no standard technology or protocol to verify and manage identities ready to be used by information systems. He described the ideal properties of such an abstract technological layer in a series of essays published in his blog in 2004 and 2005: "The Laws of Identity". These laws of identity have enlightened the path for new identity systems.

The earliest systems adopting user-password schemas put the arduous task on users, who had to remember many credentials or, more dangerously, reuse weak passwords across multiple sites, compromising security. Consequently, these systems were soon replaced by more advanced technologies influenced by those Laws of Identity. OpenID, JWT, OAuth, and other identity management protocols introduced single sign-on (SSO), token-based authentication, and federated identity. These innovations significantly improved the user experience and security of online authentication, but the W3C did not play any significant role in their design.

5.3. W3C DECENTRALISED IDENTIFIERS

---

[7] Berners-Lee, T (1999)

[8] Berners-Lee, T (1999)

[9] Berners-Lee, T (2001)

[10] Deleuze, G (1987)

The W3C's endeavours to specify a decentralised identifier only started in September 2019, when the Decentralised Identifier Working Group was formalised to specify the "W3C Decentralised Identifier" or DID. This group aimed to specify the data model and syntax of an identifier capable of enabling verifiable, decentralised digital identity. The specification was completed in July 2022 and published as a W3C Recommendation[11]. Also, in 2019, the complementary system WebAuthn was specified by the W3C to authenticate users using public-key cryptography[12].

The DID is simply a URI (similar to a web address) that associates a DID subject (the identified entity) with a DID document (data describing the subject), allowing trustable interactions associated with that subject. The DID identifies persons and organisations, things or other abstract entities. The so-called "DID controller" is the entity that can create or make changes to a DID document. By default, the DID subject is a controller of their own DID, but this is not always the case (as the goatherder may want to create a DID for the goat to recall the previous analogy). Anybody can become a DID controller, proving control over the DID without requiring permission from any other party —the DID has been designed to operate, in principle, independently of centralised registries, identity providers, and certificate authorities.

When the identified subject has an informational nature, the DID can provide the mechanism to return the DID subject itself —and all this is possible because of the cryptographic methods that can be invoked. Each DID document can include cryptographic material, verification methods, and services that facilitate the controller in proving control over the DID. Since there are multiple technologies available to implement these requirements, various *methods* are possible. These methods define how a particular type of DID and its associated DID document are created, resolved, updated, and deactivated. The specific method is, therefore, a crucial element of information for the DID. A W3C DID, which looks like this:

```
did:methodX:123456789abcdfghi
```

The first three letters are the scheme that identifies the string as a DID, and the word "methodX" is the chosen technology (more than 140 methods have been defined). The following string of characters is the method-specific identifier. Some common methods are `did:key`, used for public key cryptography or `did:ethr`, relying on the Ethereum blockchains and possibly supporting decentralised finance applications. The DID identifier is *resolvable*; that is to say, it may lead to the actual DID document, with the different attributes given to the identified subject (date and place of birth, name, etc.). Some attributes in the document are of particular relevance: who the controller is (if not the subject) and what the public key is —this enables the controller to prove ownership. The DID document is a set of RDF triples: the RDF triple is the information unit in the Semantic Web mentioned before.

5.4. W3C VERIFIABLE CREDENTIALS

The decentralised identity ecosystem of the W3C is completed with the W3C Verifiable Credential (VC)[13] specification. In this context, a credential is a digital document containing *claims* made by an *issuer* about a subject. For example, a credential issued by a university may state that I have obtained a certain degree. The university is the issuer, and I am the *holder* of the credential. As the holder, I can present this credential in a job interview when I need to demonstrate that I have such a qualification. The job interviewer may verify that claim; hence, the interviewer will be called a *verifier*. The information shown is said to be a *presentation,* that is to say, a package of one or more verifiable credentials assembled by me as a holder and shared with the verifier (the job interviewer). This simple schema is depicted in Figure 1.

[11] Sporny M (2022a)
[12] Balfanz D (2019)
[13] Sporny M (2022b)

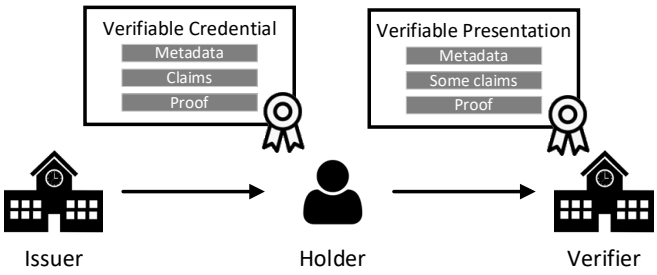

Figure 1. The simplest use of Verifiable Credentials

The beneficial property of VCs is that the presentation allows the verifier to check the validity of the credentials and the authenticity of the claims they contain. Anyone can verify the validity of a VC using the information contained within the credential itself and the referred cryptographic methods without the need for a third party; the job interviewer does not need to contact the university or check a registry. Just run an algorithm. Nowadays, university diplomas use special paper and ink to make forgery and tampering difficult; however, breaking the authenticity and integrity of cryptographically signed credentials is nearly impossible.

There is one last element missing. Additional measures may be necessary for the job interviewer to verify that the university, potentially identified with a DID, issued the VC. The university could publish its DID on a physical bulletin board, participate in a web of trust, or register with a *trust anchor*. This well-known entity would confirm the university's identity. Of course, trust anchors represent the opposite of decentralisation, as typical trust anchors are governmental bodies, accreditation organisations, or other reputable institutions. Yet, the W3C VC specification sanctions this solution with the idea of a *verifiable data registry*. A verifiable data registry is a system, decentralised or not, that serves as a trusted source of any identity-related data. Verifiable data registries are used to store and manage DIDs, DID documents, and other verifiable credentials.

In other words, a verifiable credential is a cryptographically signed message, and the W3C standard on Verifiable Credentials specifies the data structure. This data structure is simple: every credential comprises three parts: the credential metadata, the claims, and the proofs. Some metadata elements are mandatory, such as the type of claim, the claim ID, the issuer, the expiration date, or the credential subject, but adding an attribute of choice is also possible.

The specification also adheres to the Semantic Web principles described before. Thus, identifiers in a VC are URIs, strings like web addresses, many of them DIDs. Information is represented in a graph structure, possibly connected to entities out of the VC itself. This technological choice also grants that the DID and VC specification can be extended to anyone and anything, including cloud, edge, and IoT resources.

Different lifecycles for Verifiable Credentials (VCs) have been described.[14] In the archetypical case, the process begins with issuing a VC and storing the credential in a credential repository (second step). Subsequently, in the third step, one or more VCs are packaged into a verifiable presentation for verifiers. Finally, in the fourth and final step, the verifier verifies the verifiable presentation. Revocation of identifiers and credentials is also included in the specification. There are several reasons for revocations: a claim might have been made by mistake, or a private key might have been lost. A credential status property in the VC is specified to link to a status list or registry. This may be a centralised verifiable data registry or refer to information stored on a blockchain.

Credentials are, therefore, stored in credential repositories, which we usually name *digital wallets*. The role of these digital wallets is extremely important —see how the EU Digital Identity Wallet is now being introduced in Europe. Wallets must be capable of storing both VCs and the cryptographic key pairs associated with the DIDs. This capability allows users to interact with service providers without needing an internet connection, utilising Bluetooth or NFC.

5.5. W3C POLICIES

[14] Brunner C (2020)

The W3C also has a specification for representing policies, the Open Digital Rights Language (ODRL). ODRL became part of the W3C standards in 2018. A policy provides information on permissions, prohibitions and duties related to an asset. The validity of the permissions can be conditioned to the satisfaction of zero or more conditions, such as a payment. Temporal or geographical constraints are also not uncommon. The language comes with vocabulary elements to represent some typical actions that are permitted (such as *play*, *publish*, etc.) and some typical constraints (payment, spatial, temporal, etc.). The language can be extended through the specification of *profiles*, which further refine the terminology used in specific domains. ODRL policies can represent policies in force (said to be of type *Set*) but can also represent *Offers* and *Agreements*. The agreement life-cycle is not described by the recommendation, though.

Policies determine the behaviour of access control systems (that selectively grant access to media content, computer files or any other information). Still, they can also be used in various scenarios —such as compliance checking[15] or contract management.[16] ODRL has been used in various domains: in digital rights management for media content in mobile phones[17], in the news sector[18], in the language data sector[19], and lately, in the data markets called Data Spaces[20,21] or the financial data market, where the W3C Rights Automation for Market Data Community Group has specified an ODRL profile to trade with market data.

ODRL policies are represented in RDF —the Semantic Web data format—and can be easily expanded and integrated with other W3C standards. However, no formal proposal exists to use ODRL policies with decentralised identifiers and verifiable claims. A relatively novel approach for the integration of ODRL with DID and VC would be materialised in the following manner (illustrated in Figure 2):

- The ODRL policy, represented in RDF, could be one of the claims in a Verifiable Credential or a Verifiable Presentation. This integration would reinforce the policy's value, for its provenance would be guaranteed by an algorithm that can be run without the participation of the policy issuer or any other authority. The policy could be trusted because no forgery or tampering would be possible.
- The two parties in an ODRL policy are the policy assigner and the assignee. The assigner determines which rights, prohibitions, and obligations operate on a possible assignee. Policies with no assignee means they are intended for general consumption. There is no formal restriction on how these parties are referenced, and nothing prevents the policy from using DIDs. This integration would enable policies to be used in a decentralised environment.
- A DID may also identify the policy itself, which would be contained in a DID Document. This integration would solve the problems of policy identification, policy resolution (unspecified by ODRL) and policy encryption, which would now be possible.

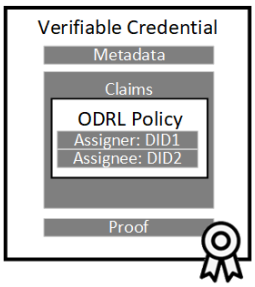

Figure 2. ODRL Policies as a part of the Verifiable Credential

[15] de Vos M (2019)
[16] Steyskal S (2015)
[17] Torres V (2008)
[18] IPTC Rights Expressions Working Group (2018)
[19] Rodríguez V (2015)
[20] Steinbuß S (2021)
[21] GAIA-X European Association for Data and Cloud (2022)

The joint use of these three W3C technologies (DID, VC, ODRL) is a novel idea that has only been sketched in the framework of data markets[22] but has not yet been implemented. The ability of ODRL to represent the exchange of rights and obligations present in every contract and the ability of DID and VC to grant integrity, confidentiality, availability, authenticity, and non-repudiation for these policies make their joint use an excellent choice in private commercial exchanges. It is also worth mentioning that all of this can be accomplished *without* blockchain technologies. Indeed, these policies or similar policies like those of MPEG-21 can work together with distributed ledger technologies and smart contracts.[23] —transforming policies into smart contracts has been standardised for the media content case as ISO/IEC 21000-23.

5.6. ANALYSIS OF WEB TECHNOLOGIES FOR DECENTRALISED IDENTITY

The applications of decentralised identifiers and verifiable credentials are unlimited. They can be used to support a birth certificate, verify the authenticity of a legal apostille, guarantee the origin of a health certificate, or certify the authenticity of some organic food—see Mazzocca et al.[24] For an exhaustive survey. The W3C has also collected some use cases in education, retail, finance, healthcare, professional credentials, legal identity, and IoT devices.[25]

The World Economic Forum acknowledged in its 2016 report on the subject matter that the importance of digital identity for the financial sector cannot be underestimated. [26] For the financial domain, five application examples are given: (i) Reuse Know Your Customer (KYC), where the KYC obligation is satisfied by using government-supplied VCs that demonstrate the customer identity; (ii) money transfers, where the receiver and sender of the money can be identified to comply with the regulations against money laundering; (iii) closing a bank account, where the mechanisms for revoking credentials come into play; (iv) data portability among financial services, where the interoperability of wallets is crucial and (v) opening a bank account, where the use of government-supplied VCs suffices to the operation in a remote modality.

Different organisations have implemented systems based on the W3C VC specification: companies like Microsoft[27] or IBM, smaller players such as Consensys[28] (with their popular products Serto / Veramo), foundations like the Sovrin Foundation or the IOTA Foundation, governments (Canada, New Zealand), universities like MIT[29] or open-source projects like Hyperledger Aries[30] or the DIDKit toolkit. These efforts demonstrate the growing adoption of W3C verifiable credentials across many industries and use cases. And indeed, one of the key sectors is Fintech. However, do these technologies announce a revolution enabling decentralised financial applications?

The technical specifications of W3C Digital Identity and Verifiable Credentials embody the principles of decentralised identity and self-sovereign identity, and their joint use in various cases presents several advantages. First, they are secure, as the authenticity of the data is algorithmically guaranteed. Second, some argue they are privacy-friendly, allowing holders to disclose only the minimum necessary information to each verifier selectively. Third, they are standards-based and interoperable across different technologies. Fourth, they enable decentralisation, potentially leaving control in the hands of users rather than centralised authorities. Finally, verifiable credentials are quite efficient, as they can be easily issued, shared, and verified —unless used in connection with blockchains.

W3C Verifiable Credentials have not been free from critiques, either. The most obvious is that in practice, the two main features of self-sovereign identity, namely, that individuals own and control their identity, are not feasible. Anyone can create a decentralised identity, but this is pseudonymous information by nature—we don't know the subject's real-world identity. Without a central registry or trust schema with a root of

[22] GAIA-X European Association for Data and Cloud (2022)
[23] Zichichi M (2023)
[24] Mazzocca C (2021)
[25] McCarron S (2019)
[26] McWaters J (2016)
[27] https://www.microsoft.com/en-gb/security/business/identity-access/microsoft-entra-id/
[28] https://www.uport.me/
[29] https://digitalcredentials.mit.edu/
[30] https://www.hyperledger.org/projects/aries

trust (e.g., Certificate Authorities), DIDs do not provide advantages over having a pseudonymous email address.

Moreover, some have doubted that decentralisation is at the heart of the specifications[31]. In the example in this Chapter, the holder and the subject of the claim were the same. But this might not always be the case, and nothing prevents the holder from being a government database the subject has no knowledge of —verifiable data registries do not need to be decentralised at all. Suspicion has been cast on the fundamental purpose of VCs, whose specification has been generously funded[32] by the Department of US Homeland Security concerning COVID-19 passports and related restrictions —see implementations such as Consensas Information Passport[33], BlockID[34] or those based on Solid[35]. If privacy is about unlinkability[36], and the Semantic Web is about linkability and data integration, something is fundamentally broken with using Semantic Web postulates on identity systems. Besides, several technical problems have been described. The standards family is incomplete, and the Verifiable Credential Data Integrity methods specification has not been finalised. The bit-serialization string of the credential is ill-defined, and software developers have identified specification gaps[37]. The resolution from a DID to the DID document differs for each method (but often on blockchains). In practice, they may resort to permissioned federations —public databases of DID documents- again against the privacy-by-default philosophy. Lack of expert review on security and lack of formal scrutiny adds to this problem.

5.7. CONCLUSION

Most of the world's population owns at least one digital identity. However, the concept of digital identity extends far beyond the authentication of human beings in online services. Identity is something more important than an invitation card. Identity is a sense of self; it is about how you perceive yourself, your values, beliefs, experiences, and relationships; it is about the internal understanding of who you are. Now, we live in the digital. Our memories are no longer disembodied, and once transformed into data, they can be processed and used by algorithms.

This chapter presents the World Wide Web Consortium and two of its latest specifications: the Decentralised Identifier and the Verifiable Credential. They promise that, as an implementation of the Self-Sovereign Identity idea, individuals will own and control the identity information. Having the technical ability to do this is already a great advance, but the chapter has also shown that, in practice, authorities will use the standards in centralised schemas.

However, the technical progress brought by these technologies is not to be disdained. The chapter also shows how to use these identifiers and credentials in conjunction with the W3C language to represent permissions, obligations, and prohibitions, known as ODRL. ODRL is already used in many sectors, and the enhanced security properties for the claims can only be a positive development.

5.8. REFERENCES

Allen C (2016) The Path to Self-Sovereign Identity. Blog posts.
https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/ Accessed 15 Jun 2024

Alzahrani B (2020) An information-centric networking-based registry for decentralised identifiers and verifiable credentials. IEEE Access 8:137198-137208.

Berners-Lee T (1999). Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor. Harper, San Francisco

[31] Halpin H (2020)
[32] Department of Homeland Security Contract HSHQDC-17-C-00019
https://www.sbir.gov/sbirsearch/detail/1302459
[33] https://github.com/Consensas/information-passport
[34] https://www.1kosmos.com/identity-management/digital-identity-in-a-covid-world/
[35] Eisenstadt M (2020)
[36] Pfitzmann A (2010)
[37] Alzahrani B (2020)

Berners-Lee T, Hendler J, Lassila O (2001) The Semantic Web. Sci. Am. 284(5): 34–43

Brunner C, Gallersdörfer U, Knirsch F, Engel D, Matthes F (2020) DID and VC: Untangling decentralised identifiers and verifiable credentials for the web of trust. In Proceedings of the 2020 3rd Int. Conf. on Blockchain Technology and Applications, Xi'an, 14-16 Dec 2020

Cameron K (2005) The Laws of Identity. Kim Cameron's Identity Weblog. www.identityblog.com/?p=352. Accessed 15 Jun 2024

Deleuze G, Guattari F (1987) A thousand plateaus: Capitalism and schizophrenia. University of Minnesota, Minneapolis

Eisenstadt M, Ramachandran M, Chowdhury N, Third A, Domingue J (2020) COVID-19 antibody test/vaccination certification: there's an app for that. IEEE Open Journal of Engineering in Medicine and Biology, 1:148-155.

GAIA-X European Association for Data and Cloud (2022) Gaia-X Architecture Document 22.04 Release. Gaia-X European Association for Data and Cloud AISBL.

Halpin H (2020) Vision: A critique of immunity passports and W3C decentralised identifiers. In Security Standardisation Research: 6th International Conference, Springer International Publishing, London, 30 Nov – 1 Dec 2020.

Steinbuß, S. (2021) Usage Control in the International Data Spaces. International Data Spaces Association, https://doi.org/10.5281/zenodo.5675884, Accessed 15 Jun 2024

IPTC Rights Expressions Working Group (2018) IPTC RightsML Standard 2.0, International Press Telecommunications Council

Mazzocca C, Acar A, Uluagac S, Montanari R, Bellavista P, Conti, M (2024) A Survey on Decentralised Identifiers and Verifiable Credentials. arXiv preprint arXiv:2402.02455

McCarron S et al. (2019) Verifiable Credentials Use Cases W3C Working Group Note 24 September 2019

Ianella R, Villata, S (2018a) ODRL Information Model 2.2. W3C Recommendation 15 February 2018

Ianella R, Steidl M, Myles S, Rodríguez-Doncel V (2018b) ODRL Vocabulary & Expression 2.2. W3C Recommendation 15 Feb 2018

Pellegrini T, Schönhofer A, Kirrane S, Steyskal S, Fensel A, Panasiuk O, Polleres A (2018) A genealogy and classification of rights expression languages-preliminary results. In Data Protection/LegalTech. Proceedings of the 21st International Legal Informatics Symposium, IRIS, Vienna, 14 Feb 2018

Pfitzmann A, Hansen M (2010) A terminology for discussing privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf In TU Dresden, Accessed 15 Jun 2024

Preukschat A, Reed D (2021) Self-sovereign identity. Manning Publications, Shelter Island

Rodríguez-Doncel V, Labropoulou P (2015) Digital Representation of Rights for Language Resources. In Proc. of the 4th W. on Linked Data in Linguistics: Resources and Application, Association for Computational Linguistics, Beijing, 31 Jul 2015

Sporny M, Guy A, Sabadello M, Reed D (2022a) Decentralised Identifiers (DIDs) v1.0 Core architecture, data model, and representations. W3C Recommendation 19 July 2022

Sporny M, et al. (2022b) Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022

Steyskal S, Kirrane S (2015) If you can't enforce it, contract it: Enforceability in Policy-Driven (Linked) Data Markets. In Semantics (posters & demos), Vienna, 16-17 Sep 2015

De Vos M, Kirrane S, Padget J, Satoh K (2019) ODRL policy modelling and compliance checking. In Rules and Reasoning: Third International Joint Conference, RuleML+ RR 2019, Springer International Publishing, Bolzano, 16-19 Sep 2019

Tobin A, and Reed D (2016) The inevitable rise of self-sovereign identity. The Sovrin Foundation, 29 (2016):18

Torres V, Serrao C, Dias J, Delgado J (2008) Open DRM and the Future of Media. Open DRM and the future of media 2:28-36.

Balfanz D et al. (2019) Web Authentication: An API for accessing Public Key Credentials Level 1. W3C Recommendation, 4 March 2019

McWaters J. et al. (2016) A Blueprint for Digital Identity. World Economic Forum Future of Financial Services Series. https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf Accessed 15 Jun 2024

Zichichi M, Ferretti S, Rodríguez-Doncel V (2022) Decentralized personal data marketplaces: How participation in a DAO can support the production of citizen-generated data. Sensors 22(16): 6260.

Zichichi M, Rodriguez-Doncel, V (2023) Encoding of Media Value Chain Processes Through Blockchains and MPEG-21 Smart Contracts for Media. IEEE MultiMedia, 22:1-8