BLOCKCHAIN™ IN HEALTHCARE TODAY

DISCUSSION

A Proposal for Decentralized, Global, Verifiable Health Care Credential Standards Grounded in Pharmaceutical Authorized Trading Partners

Victor Dods and Ben Taylor*

LedgerDomain, Las Vegas, NV, USA

Abstract

The twin forces of privacy law and data breaches have fundamentally challenged how we collect, store, and share sensitive information. Within this landscape, healthcare information is sacrosanct – and intimately tied to identity and data ownership. Building on prior work with UCLA Health, Genentech (a member of the Roche Group), Sanofi, Amgen, Biogen, and others, we offer this opinion piece to promote the development of a standard for decentralized Verifiable Credentials (VCs). This will empower Authorized Trading Partners (ATPs) in the pharmaceutical supply chain to trade and exchange information in compliance with the US federal law. Starting with credentialing and interoperability for the ATP community, our ultimate goal was to chart a path to a global standard for all health care VCs – providing individuals and health-care professionals control over their own data. By sharing our results and releasing essential components of the work to the public domain, we hope to align and connect with other foundational efforts, thus evolving standards within a truly open framework with broad stakeholder involvement.

Keywords: *verifiable credentials*; *identity*; *DSCSA*; *pharmaceutical supply chain*; *interoperability*

Received: 23 February 2021; Accepted: 18 March 2021; Published: 28 April 2021

The rise of COVID-19 and the Solarwinds hack have exposed deep and systemic vulnerabilities in our health-care system (1).[1] As the world converges around solutions to the pandemic, 'the largest and most sophisticated [cyber]attack the world has ever seen' remains largely unresolved. Both have far-reaching implications on how we prevent and mitigate future crises.

Back in our school days, the janitor had a big key ring that provided access to any office or drawer. If that key ring was held by somebody with bad intentions, bad things could happen. This is the case today with any system that manages your identity on your behalf, including government systems and technology enterprises. The administrator always has a backdoor (3, 4). By contrast, in a decentralized system you decide who holds your private key.[2]

While governments, privacy advocates, and security professionals redraw the lines around anonymity and data protection (5), personal health care information remains sacrosanct. Just as the Solarwinds hack provoked important questions about information security practices, so we must ask whether there is any rationale to centrally administer personal health care information. We assert the answer is No.

The time has come for *self-sovereign health-care privacy*, in which individuals and health-care professionals have some measure of control over their data and identities with their own private credentials (6). This provides the bedrock for stakeholders to carry only their own data

1 For instance, as the COVID-19 Credentials Initiative wrote in its hello world, 'without a holistic perspective from the onset, many COVID-19 technology solutions may introduce unintended results (e.g. surveillance, abuse of personal data, social inequalities). In order to avoid such outcomes, we have committed ourselves to open collaboration with a diverse range of experts, embracing open standards, and protecting the fundamental privacy and personal data rights of all stakeholders' (2).

2 With Bitcoin, you can hold your own wallet, or you can hire and fire Coinbase. Either way, you are in control.

*Correspondence: Ben Taylor. Email: ben.taylor@ledgerdomain.com

 Citation: Blockchain in Healthcare Today 2021, **4**: 175 - http://dx.doi.org/10.30953/bhty.v4.175

and leverage authenticated identities, interacting safely with select parties of their interest. This would impact everything from drug supply assurance to cell and gene therapies and clinical studies, not to mention the needs of underserved communities.

The need for ATP VCs

While health care is an enormously diverse and complex ecosystem, the secure and interoperable management of identity and private data is a common challenge.[3] The starting point in our effort to address this lies in an emergent class of identities with relatively clear boundaries and a strong motivating use case: Authorized Trading Partners (ATPs) as defined by statute in the US pharmaceutical supply chain.

The Drug Supply Chain Security Act (DSCSA) imposes particular requirements on five groups ('entity types') of stakeholders: manufacturers, repackagers, wholesale distributors, third-party logistics providers (3PLs), and dispensers (e.g. pharmacies) (11). One such requirement is an extended 'know your customer' rule, according to which each ATP is required to confirm that their trading partners are also authorized. In many cases, the law requires interactions between entities without any direct business relationship.[4]

To enable near-real-time interoperability within the ATP community, stakeholders have identified the value[5] of decentralized ledger technologies (DLTs), such as blockchain and decentralized identifiers (DIDs). Together they provide all parties with a 'single source of truth' to address challenges, such as master data management and counterfeit detection.[6] At a more fundamental level, ATPs must be able to identify other ATPs using VCs for compliant transactions and information disclosures; the same necessity motivated the development of the eXtended Authorized Trading Partner (XATP) framework (16, 17).

Any framework addressing this challenge must satisfy the following two requirements:

1. It must prove that a given credential holder is a valid and current ATP of a given ATP entity type, and

2. It must provide mechanisms to comply with privacy laws, such as GDPR and the California Privacy Act (CalPrivacy), which concerns personally identifiable information (PII).

To realize this mission, a coalition of stakeholders must come together to provide interoperable tooling.

Collaborative proposal for a common ATP VC standard

Our vision is an *interoperable system employing cryptographic schemes, which allow for the selective disclosure of credential elements*. There is also a need for interoperability regarding workflows mandated by law.[7] The W3C VC Data Model (17) presents a flexible and extensible credential scheme leveraging decentralized identifiers (DIDs),[8] which meet the needs of ATPs.[9,10] In this case, we propose an ATP-specific scheme anchored in W3C standards, which would allow interoperation between all ATP software solutions.[11]

To chart the path of an ATP VC standard, several key questions must be addressed by stakeholders.[12] These, in turn, provoke further questions around implementation, which can be broadly divided into software and non-software domains.

Key questions

1. Who are the stakeholders (ATP entities, relevant governance groups, solution providers, and accreditors)?[13]

3 Other foundational efforts to develop and deploy credentials for health care include the Vaccination Credential Initiative (7), Decentralized Identity Foundation (8), CommonPass by The Commons Project and The World Economic Forum (9), and the SMART Health Cards Framework (10). Our aim is to bring together stakeholders to address an ATP-specific W3C VC scheme, and look towards interoperability and expansion.

4 Under certain circumstances, drug packages are required to be verified with the manufacturer or repackager in order for transactions to proceed. One such circumstance is the saleable returns process, in which dispensers with surplus drug return the drug to their wholesaler, or sell it to another ATP. This process represents 2–3% of the overall volume of the US pharmaceutical supply chain, or 59 million units annually (12). Manufacturers and dispensers typically have no former business relationship; yet, there must be a framework for these parties to interact within the broader requirements of the 'fully electronic, interoperable system' (13) mandated by the law.

5 'Data-informed technologies, such as distributed ledger solutions like blockchain, will be critical to support FDA's track-and-trace priorities' (14).

6 Much of this effort would not be possible without the near-universal adoption of the GS1 DSCSA standard (15) within the US pharmaceutical supply chain. While there are many hurdles in standards development and adoption, we believe that alignment can be more rapidly achieved in well-defined communities with clear and present needs.

7 By its nature, interoperation implies authentication and the corresponding need for a mutually understood credential scheme, which allows each ATP's software to verify the validity of transactors within the ecosystem.

8 A portable URL-based identifier associated with an entity, most often used in VCs. They allow VCs to be easily ported from one repository to another without the need for reissuing the credential (18, 19).

9 The extensibility of the W3C VC data model comes in the form of allowing context-specific credential definitions, a natural complement to DIDs.

10 Beyond the healthcare ecosystem, W3C DIDs have also seen adoption by the international technology standards organization Object Management Group (20) and the Sovrin Foundation (21).

11 These ideas may justifiably be termed 'old wine in new bottles', but collective security and interoperability always improve as more parties adopt and then adhere to best security practices. At the same time, we are certainly not discouraging any ongoing efforts to bolt W3C credentials onto identity systems that are anchored in traditional centralized registries. These efforts can certainly enhance interoperability, but it should nonetheless be noted that they neither support privacy nor address those systems' inherent single points of failure. (Painting spots on a house cat doesn't make it a leopard!)

12 As different ATP entities will have a stake in different parts of the standard, participation in the standard development should reflect those roles.

13 The FDA is a key indirect stakeholder, but best practice is for regulators to work through ATPs to avoid creating a single point of failure.

Citation: Blockchain in Healthcare Today 2021, **4**: 175 - http://dx.doi.org/10.30953/bhty.v4.175

2. What are the stakeholders' workflows?[14]
3. What workflows will be, or are likely to be, needed for compliance with future laws?
4. What are the requirements do those workflows impose on the VCs?[15]
5. How best to develop standards needed to meet those requirements?

Non-software implementation

1. **What should the trust model be?** In other words, how does a verifier determine who is authorized to issue ATP credentials? This might take one of two forms:
    a. **A hierarchical Public Key Infrastructure (PKI)** architecture supported by the U.S. Department of Health and Human Services (HHS), Food and Drug Administration (FDA), National Institute of Standards and Technology (NIST), a consortium of ATPs, and other stakeholders (such as PDG (24)) defining the trust anchors[16] for issuing credentials to ATPs.[17] This would be less fragile for purposes of VC verification, but would still require a central authority (or consortium) to define the trust anchors.
    b. **Choose your own trusted authorities** where each organization defines its own trust anchors (perhaps based on some minimal as-needed whitelisting). This would be more fragile for purposes of VC verification, but would not require a central authority (or consortium) to define the trust anchors.
2. **For each ATP type and its delegates, what is needed in the VC to meet the workflow needs of different organizations?**
    a. Which schema defines what a VC looks like for each ATP?
    b. What are the rules and requirements for how an ATP can be issued a VC?
    c. What are the rules and requirements for a company to be an issuer of VCs?
    d. What are the presentation requirements for VCs?
        i What are the contexts that require a presentation?[18]
        ii Which claims must be shown in each context?[19]
        iii Which cryptographical model is acceptable to participants (e.g. ECDSA vs. pairing-based crypto with zero-knowledge proofs (ZKPs))?
        iv What are acceptable methods of revocation checks (e.g. ZKPs, Bit-vectors, and Certificate chains)?
    e. Which formats are mandated, and which are acceptable (e.g. BARE message format (binary), JSON-LD, and JWT)?
    f. Which systems will be used to create presentations and accept them?
3. **What are the rules and requirements for defining where schemas, identifiers, and keys can be stored and secured?[20]**
4. **Which schema will define what a VC looks like for drug provenance?**
5. **How is this system bootstrapped?**
6. **How does a new ATP in the space become certified?**
7. **Which are capabilities needed regarding the hiding or minimizing revelation of PII, especially with respect to relevant privacy laws, such as GDPR and CalPrivacy?**

Software implementation

1. What is the scope of interoperability with different W3C-VC-compliant formats?[21]
2. How many different cryptographic schemes need to be supported by each ATP VC implementation?[22]

14 The XATP application framework incorporates one potential workflow for an enhanced verification. Because this involves interaction between dispensers and manufacturers, particular emphasis has been placed on credentialing for those entity types (16, 17). A credentialing model for dispensers is currently in place, with manufacturer credentialing on the roadmap.

15 Given the need for protecting PII and minimizing its disclosure, we recommend that the ATP VC use a cryptographic scheme, which allows zero-knowledge proofs and selective disclosure. In particular, we recommend the use of BBS+ signatures, which allow a flexible and minimal disclosure of information in credentials (22), thus enabling compliance with data privacy laws and best practices, while still providing powerful and meaningful credentials. BBS+ is a cryptographic signature across multiple messages that also support selectively disclosing any subset of messages, while the remainder are withheld when presented to a relying party. The implementation is written in Rust in Hyperledger Ursa, which supports compiling to mobile devices, servers, and WebAssembly (23).

16 'An authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative" (25).

17 A precedent for this is Mozilla's approach (26).

18 For example, drug receipt, returns, and master data access.

19 'A verifiable claim is a qualification, achievement, quality, or piece of information about an entity's background, such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity which establish its existence and uniqueness' (27). Claims can be grouped into 'bundles'. For example, a pharmacist requesting drug verification from a manufacturer would present a bundle, indicating that they are a currently licensed pharmacist *and* a pharmacist in charge at a particular pharmacy. Together, the DID and the bundle of claims constitute a VC. We may assume that the higher the stakes, the more claims must be revealed in the presentation of the VC.

20 In the case of XATP, identity information is held on the user's mobile device instead of the service, and control over the identity lies with the keys stored in the device (16, 17).

21 JSON has emerged as a widely used data format, including JWT-based VCs used by Spherity's ATP VCs (28), and JSON-LD-based VCs, which are generally recommended by the W3C VC data model and employed by the COVID-19 Credentials Initiative hosted by Linux Foundation Public Health (29). Alternatively, a compact, binary encoding scheme (such as protobufs [30]) might be preferred in many machine-to-machine workflows, with JWT/JSON-LD employed for interoperability between organizations (29).

22 The schema for W3C VCs (32) specifies four digital signature schemes. For the purpose of minimizing PII revelations, we are exploring the use of ZKPs and selective disclosure. It should be noted that ZKP imposes certain restraints on the data structure of attributes, requiring mapping nested content to a list (31).

3. Which mechanisms for credential revocation would be mandated or supported?[23]
4. How shall guidance and resources for creating a compliant ATP VC implementation be developed?
5. What are the specifications for test cases and test environments for verifying compliance of an ATP VC implementation?[24]

For a standard to be adopted, the VC should not be a 'black box'. There should be sufficient transparency for understanding how issuance and verification work, the context necessary for VC usage and a path to including a possible human in the loop.[25]

Recommendations and next steps

Within the ATP context, many of the key questions raised by this paper have already been partially resolved by stakeholders joining together to define a trust framework and governance structure (35, 36).[26]

This proposed solution is a complete, fully transparent, open-source reference implementation that satisfies the requirement for interoperability across all ATP types. We are looking to work with a coalition of the willing to design and contribute key components of this effort, including an initial implementation that should be adequate for everyday use and upgradeable over time.

Technical considerations

- We see the overall effort constituting the definition of a global ATP schema and development of a reference implementation, which will be entirely open source and include protocols for revocation.
- We believe that the schema should be global, in that the contents of an ATP VC should be global, but that different formats for representing the VC should be allowed.[27]
- As a strawman, we suggest that a reference implementation should be done in Rust with a GoLang wrapper (standard) and a WebAssembly wrapper (desired).[28]
- We do not see any need for anchoring standards, so a diversity of anchoring points (e.g. Ethereum or Sovrin) should be acceptable. Similarly, using an X509 DID method to hook into existing web PKI for trust anchors should be acceptable (39).
- We support technical decisions that are future proof.

Governance considerations

- Any role-based privilege supported by a VC should be factually grounded and accredited under a trust framework with well-defined governance.[29]
- We believe that the global schema should ultimately be an ISO standard. As for the ATP schema itself, November 2022 should be targeted, as the interoperability requirements take full effect by November 2023.
- The reference implementation should be released under an open-source license (e.g. Apache 2), and it should be open to global collaboration.

Much as a driver's license has become a standard form of physical identification outside its original use case, so a VC schema grounded in the ATP community would address a stipulated need within the US pharmaceutical supply chain, while also having far-reaching implications for other health care domains. We aim for a future in which the VC schema developed for ATPs could be seamlessly extended to other open-source credentials to serve patients, caregivers, and all participants in the health-care system.

In the same world, patients could then share VC-backed laboratory results and prescriptions with pharmacies and clinics.[30] Due care would be needed in adherence to best practices as promulgated by HIPAA, GDPR, and CalPrivacy, so that patients carry only their own data[31] and disclose it to select parties of their choice. A secure, interoperable, and privacy-preserving world would mean lower costs, better care outcomes,

23 There is only some high-level guidance in the VCs' Data Model.
24 For example, each ATP VC vendor could provide their own 'test network' (or instructions for how to run one locally, in the case of open source implementation) against which denizens of the ATP software-verse can test their code.
25 For instance, easy discovery of the ATP's website or other relevant contact information. JSON-LD is a good candidate for this purpose as it enables clients to uncover linked data based on a principle known as Follow Your Nose (33).
26 These include the Internet Identity Workshop headed by Doc Searls, Phil Windley, and Kaliya Young (34), and more recently Sovrin Foundation, Spherity, the Center for Supply Chain Studies, and the FDA's DSCSA Pilot Project Program.
27 Note that for much of this article, we discuss VCs for ATP entities, which may be distinguished from a personal VC that specifically relates to a person's identity (e.g. equivalent to their driver's license and containing their personal information). A pharmacist might have an ATP pharmacist credential that attests to his or her pharmacist license number, validity date, and other details that would not contain unrelated identity information, such as their home address. There are also VCs for entities meant for automated systems, such as authentication systems and server backends.
28 WebAssembly (Wasm) is an assembly-like language with a compact binary format that runs with near-native performance and provides languages, such as C/C++, C#, and Rust with a compilation target, so that they can run on the web (37). In 2019, the specification became a W3C recommendation (38), and as such, may have particular applicability to interoperability. Given that WebAssembly is the avenue for compiled code to run within the browser, at the very minimum, a WebAssembly port of the open-source solution should provide a means to easily verify VCs from within the browser. However, with regard to holding and issuing credentials, the browser is inherently less secure than non-browser platforms, and thus, poses additional challenges.
29 Within a trust framework model, the governance layer establishes business, legal, and technical policies, and manages membership and participation. Governance is typically handled by organizations created by constituent members to administer the activities associated with operating an identity federation. They may be government programs, corporate entities, not-for-profit membership organizations, or industry associations (38, 40).
30 This change simply digitizes the information movement currently achieved by paper. Paper versions of credentials can still be given simultaneously until on-the-ground workflows adapt to the new VCs.
31 For principles concerning the use of biometrics within a self-sovereign identity solution, see Callahan et al. (41).

Citation: Blockchain in Healthcare Today 2021, **4**: 175 - http://dx.doi.org/10.30953/bhty.v4.175

greater rate of clinical innovation, and an abundance of opportunity for private companies to add value by leveraging the schema.

Over the coming weeks and months, we will be working with stakeholders in the health care and identity space to chart the best path forward for ATP W3C VCs, and beyond. In the interest of public and transparent conversation, specific schemas, supporting documentation, and updates to this effort will be published at Zoogma.org.

Acknowledgements

Authors would like to personally thank Mike Lodder for his insights regarding DIDs and cryptographic schema. The authors would also like to thank Brian Behlendorf (Linux Foundation); Connie Jung, RPh, PhD (FDA's Center for Drug Evaluation and Research); Melanie Nuce, Gena Morgan, and Peter Sturtevant (GS1); Eric Marshall (Partnership for DSCSA Governance); Bob Celeste (Center for Supply Chain Studies); and Max Sills, JD.

The authors would also like to acknowledge the XATP Working Group for their contributions to the framework that informed this proposal. These include Ghada L. Ashkar, Pharm, Kalpan S. Patel, PharmD, MBA, and Josenor de Jesus, PharmD, MBA, FACHE (UCLA Health); Vidya Rajaram, Mark Karhoff, Nirmal Annamreddy, and Kathy Daniusis (Genentech, a member of the Roche Group); Nikkhil Vinnakota, Natalie Helms, and Alina Grigorian (Amgen); Arthi Nagaraj (Sanofi); Greg Plante (IQVIA); Todd Barrett, RPh (Providence Health); and Ben Nichols, Will Jack, and Will Chien, PharmD, MBA (LedgerDomain). The foregoing acknowledgements do not imply consensus nor endorsement.

Conflict of interest and funding

The authors declare no potential conflicts of interest. This proposed study represents the views of the authors and has no external funding.

Contributors

Both authors contributed to the conception, development, and writing of the proposal. Victor Dods led the technical considerations and recommendations around DIDs and cryptographic schema.

References

1. Heath B. SolarWinds hack was 'largest and most sophisticated attack' ever – Microsoft president [Internet]. Financial Post; 2021 [cited 22 February 2021]. Available from: https://financialpost.com/pmn/business-pmn/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president
2. COVID-19 Credentials Initiative. Hello world from the COVID-19 credentials initiative [Internet]. Medium; 2020 [cited 22 February 2021]. Available from: https://cci-2020.medium.com/hello-world-from-the-covid-19-credentials-initiative-6d45534c4b3a
3. Bossert TP. I was the homeland security adviser to Trump. We're being hacked [Internet]. The New York Times; 2020 [cited 22 February 2021]. Available from: https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html
4. Krebs B. At least 30,000 U.S. organizations newly hacked via holes in Microsoft's email software [Internet]. Krebs on Security; 2021 March 5 [cited 18 March 2021]. Available from: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software
5. Newton C. Warning signal: the messaging app's new features are causing internal turmoil [Internet]. The Verge; 2021 [cited 22 February 2021]. Available from: https://www.theverge.com/platform/amp/22249391/signal-app-abuse-messaging-employees-violence-misinformation
6. Tobin A, Reed D. The inevitable rise of self-sovereign identity [Internet]. Sovrin Foundation. 2017 [cited 22 February 2021]. Available from: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
7. Commons Project Foundation, MITRE, and Evernorth. Broad coalition of health and technology industry leaders announce vaccination credential initiative to accelerate digital access to COVID-19 vaccination records [Internet]. Business Wire. 2021 [cited 22 February 2021]. Available from: https://www.businesswire.com/news/home/20210114005294/en/Broad-Coalition-of-Health-and-Technology-Industry-Leaders-Announce-Vaccination-Credential-Initiative-to-Accelerate-Digital-Access-to-COVID-19-Vaccination-Records
8. Decentralized Identity Foundation. DIF – Decentralized Identity Foundation [Internet]. 2021 [cited 22 February 2021]. Available from: https://identity.foundation/
9. CommonPass [Internet]. The commons project. 2021 [cited 22 February 2021]. Available from: https://thecommonsproject.org/commonpass
10. Computational Health Informatics Program. SMART health cards framework [Internet]. 2021 [cited 22 February 2021]. Available from: https://smarthealth.cards/
11. U.S. Department of Health and Human Services Food and Drug Administration, identifying trading partners under the drug supply chain security act: guidance for industry – draft guidance [Internet]. 2017 [cited 22 February 2021]. Available from: https://www.fda.gov/files/drugs/published/Identifying-Trading-Partners-Under-the-Drug-Supply-Chain-Security-Act-Guidance-for-Industry.pdf
12. Healthcare Distribution Alliance (HDA). HDA saleable returns pilot study identifies two recommendations to meet 2019 DSCSA requirements [Internet]. Healthcare Distribution Alliance (HDA). 2016 [cited 22 February 2021]. Available from: https://www.hda.org/news/2016-11-10-hda-pilot-results-revealed
13. U.S. Department of Health and Human Services Food and Drug Administration. Drug Supply Chain Security Act (DSCSA) [Internet]. U.S. Department of Health and Human Services Food and Drug Administration [updated 2019 May 22; cited 22 February 2021]. Available from: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa
14. U.S. Department of Health and Human Services Food and Drug Administration. FDA's Technology Modernization Action Plan (TMAP) [Internet]. 2019 [cited 22 February 2021]. Available from: https://www.fda.gov/media/130883/download
15. GS1 US. GS1 standards resources for DSCSA implementation support [Internet]. GS1 US; 2021 [cited 22 February 2021]. Available from: https://www.gs1us.org/industries/healthcare/standards-in-use/pharmaceutical/dscsa-resources

16. XATP Working Group. Framework for eXtended ATP authentication, enhanced verification, and saleable returns documentation [Internet]. Las Vegas, NV: LedgerDomain; 2020 [cited 4 February 2021]. Available from: https://www.xatp.org/whitepaper
17. Ashkar GL, Patel KS, de Jesus J, Vinnakota N, Helms N, Jack W, et al. Evaluation of decentralized verifiable credentials to authenticate authorized trading partners and verify drug provenance. BHTY [Internet] 2021 [cited 18 March 2021]; 4. doi: 10.30953/bhty.v4.168
18. Sporny M, Longley D, Chadwick D. Verifiable credentials data model 1.0 [Internet]. W3C Working Group. W3C; 2019 [cited 22 February 2021]. Available from: https://www.w3.org/TR/vc-data-model/
19. Reed D, Zundel B. What are Decentralized Identifiers (DIDs)? [Internet]. SlideShare; 2019 [cited 22 February 2021]. Available from: https://www.slideshare.net/Evernym/what-are-decentralized-identifiers-dids
20. Object Management Group. Object management group issues request for information for disposable self-sovereign identity standard [Internet]. Object Management Group; 2021 [cited 22 February 2021]. Available from: https://www.omg.org/news/releases/pr2021/01-21-21.htm
21. Lodder M, Hardman D. Sovrin DID method specification [Internet]. Sovrin Foundation; 2021 [cited 22 February 2021]. Available from: https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html
22. Looker T, Steele O. BBS + signatures 2020 draft community group report [Internet]. W3C Community Group; 2021 [cited 22 February 2021]. Available from: https://w3c-ccg.github.io/ldp-bbs2020/
23. Hyperledger Ursa. GitHub [Internet]; 2021 [cited 18 March 2021]. Available from: https://github.com/hyperledger/ursa
24. USFDA. Drug Supply Chain Security Act Public-Private Partnership [Internet]. FDA: 2021 [cited 15 April 2021]. Available from: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/drug-supply-chain-security-act-public-private-partnership
25. Housley R, Ashmore S, Wallace C. Trust anchor format [Internet]. Internet Engineering Task Force (IETF); 2010 [cited 22 February 2021]. Available from: https://tools.ietf.org/html/rfc5914
26. Thayer W. Why does Mozilla maintain our own root certificate store? [Internet]. Mozilla Security Blog. Mozilla; 2019 [cited 22 February 2021]. Available from: https://blog.mozilla.org/security/2019/02/14/why-does-mozilla-maintain-our-own-root-certificate-store/
27. Otto N, Lee S, Sletten B, Burnett D, Sporny M, Ebert K. Verifiable credentials use cases [Internet]. W3C Working Group. W3C; 2019 [cited 22 February 2021]. Available from: https://www.w3.org/TR/vc-use-cases/
28. Spherity. Entities [Internet]. Spherity; 2021 [cited 22 February 2021]. Available from: https://docs.spherity.com/spherity-api/verifiable-credentials-api/entities
29. 2021.02.17 General Meeting Agenda – Healthcare SIG [Internet]. Hyperledger Foundation; 2021 [cited 22 February 2021]. Available from: https://wiki.hyperledger.org/display/HCSIG/2021.02.17+General+Meeting+Agenda
30. Google. Protocol buffers – Google's data interchange format [Internet]. GitHub; 2008 [cited 22 February 2021]. Available from: https://github.com/protocolbuffers/protobuf
31. Young K. Verifiable credentials flavors explained. COVID-19 Credentials Initiative; 2021 [cited 22 February 2021]. Available from: https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf
32. Untitled code sample. W3C working group. W3C [cited 22 February 2021]. Available from: https://www.w3.org/2018/credentials/v1
33. Dodds L, Davis I. Follow your nose [Internet]. Linked Data Patterns. 2012 [cited 22 February 2021]. Available from: https://patterns.dataincubator.org/book/follow-your-nose.html
34. Searls D. New hope for digital identity. Linux J [Internet]; 2017 [cited 22 February 2021]. Available from: https://www.linuxjournal.com/content/new-hope-digital-identity
35. Temoshok D, Abruzzi C. Developing trust frameworks to support identity federations [Internet]. National Institute of Standards and Technology; 2018. doi: 10.6028/NIST.IR.8149
36. Makaay E, Smedinghoff T, Thibeau D. Trust frameworks for identity systems [Internet]. Open Identity Exchange (OIX); 2017. Available from: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf
37. WebAssembly [Internet]. Mozilla Developer Network (MDN) Web Docs; 2021 [cited 18 March 2021]. Available from: https://developer.mozilla.org/en-US/docs/WebAssembly
38. Rossberg A. WebAssembly core specification [Internet]. W3C Working Group. W3C; 2019 [cited 18 March 2021]. Available from: https://www.w3.org/TR/wasm-core-1/
39. Kaptijn B, Gort S, Stöcker C. X.509 DID method [Internet]. Web of Trust Info. GitHub; 2019 [cited 22 February 2021]. Available from: https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/X.509-DID-Method.md
40. Sovrin Governance Framework Working Group. Sovrin governance framework V2. Sovrin Foundation; 2019 [cited 22 February 2021]. Available from: https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf
41. Callahan J, Vescent H, Young K, Duane D, Appelcline S, Othman A, et al. Six principles for self-sovereign biometrics. Web of Trust Info. GitHub; 2019 [cited 22 February 2021]. Available from: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/Biometrics.md

Citation: Blockchain in Healthcare Today 2021, **4**: 175 - http://dx.doi.org/10.30953/bhty.v4.175