Decentralized Authentication for Web of Things: a Self-Sovereign Identity (SSI)-based solution

Biagio Boi
dept. of Computer Science
University of Salerno
Fisciano, Salerno, Italy
bboi@unisa.it

Christian Esposito
dept. of Computer Science
University of Salerno
Fisciano, Salerno, Italy
esposito@unisa.it

***Abstract*—As the Internet of Things (IoT) continues to expand its reach, encompassing a vast array of devices and applications, including mission-critical ones, the need for secure and privacy-aware solutions increases. Traditional centralized authentication mechanisms may not be suitable for the highly distributed and heterogeneous nature of IoT environments, and they also have a very high demand in terms of energy and memory, which does not match the availability of resource-constrained devices. In this study, we suggest a novel solution to these difficulties based on Self-Sovereign Identity (SSI) principles, while taking into account the innovative Web of Things (WoT) architecture. It discusses how these elements from SSI can be applied in a WoT environment to establish trust between devices, users, and applications. Additionally, the paper explores the potential challenges and opportunities of integrating SSI into the WoT ecosystem, such as scalability, interoperability, and authentication. Through a comprehensive analysis of the SSI paradigm and its applicability in the WoT context, this paper sheds light on the transformative potential of device-centric identity management. It underscores the importance of privacy, security, and individual control in an increasingly interconnected world, advocating for SSI as a solution that aligns with the values of the digital age. By embracing SSI, stakeholders in the WoT ecosystem can ensure a more secure and trustworthy environment for all parties.**

***Index Terms*—IoT, WoT, SSI, Authentication**

I. Introduction

The Internet of Things (IoT) is composed of a vast number of devices exchanging a high volume of data and supports complex applications using advanced ICT solutions, including artificial intelligence, and the digital transformation of various industrial scenarios, resulting in an interconnected environment where devices, data, and people interact seamlessly. IoT-enabled applications are at the core of key industrial and societal process, which are intrinsic mission-critical, and exposes stringent security requirements. The open nature of the IoT and the pervasive deployment of devices in public spaces make protection from malicious activities very challenging. Edge device security and privacy are required to prevent probable attacks on their running applications, but also to avoid propagation to external cloud services and systems. The growing number of applications raises the necessity for CIA-tested guarantees, and the ISO/IEC 27400:2022 and other similar ones [1] present guidelines on assessing risks, and propose controls for security and privacy of Internet of Things (IoT) solutions.

Web of Things (WoT) [2] proposes standardized interactions with smart devices by creating a strong architecture centered on web-based protocols. WoT-based solutions are able to offer increased data integrity while enhancing the availability of resources. The same cannot be said for confidentiality, which is left in the background in this architecture definition. WoT identifies the devices using a Thing Descriptor (TD) [3], which contains the relevant information for interacting with the device, as depicted in Figure 1. Security is managed using the *security* and *securityDefinitions* properties. Such properties define the authentication that must be used for communicating with the IoT device. However, TD Interception and Tampering can be applied if a secure channel is not established by the parties prior to that data exchange, as stated by security consideration in Section 10 of [3]. The majority of IoT Security strategies (60% of the surveyed solutions in [4]) are related to the authentication algorithms, while encryption and secure routing strategies are placed in the background. Among them, over 55% use lightweight algorithms to reduce power and memory consumption. Considering the relevance of authentication, also within the WoT context, the implementation of these techniques assumes an important role.

Amidst this technological evolution, traditional identity management systems struggle to maintain security, privacy, and user control. The IoT devices have a lot of constraints and usually, centralized solutions are implemented in order to reduce the power consumed while having a discrete level of security. Anyway, there are hazards associated with these solutions. For example, the present centralized authentication servers may have weak authentication and restricted scalability, creating a single point of failure [5]. Moreover, in the IoT-based application, we do see password-based authentication still used, and representing a first issue for IoT security according to OWASP Internet of Things (IoT) Top 10 2018 (see https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf). Self-Sovereign Identity (SSI) offers a promising alternative by placing individuals at the center of their digital identities and exploiting a password-less solution that is more robust to possible attacks. It enables users to assert, own, and control their identity attributes without reliance on centralized authorities. By leveraging cryptographic principles and decentralized ledger technologies, SSI

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

```
{
    "@context": "https://www.w3.org/2022/wot/td/v1.1",
    "id": "urn:uuid:0804d572-cce8-422a-bb7c-4412fcd56f06",
    "title": "MyExampleThing",
    "securityDefinitions": {
        "basic_sc": {"scheme": "basic", "in": "header"}
    },
    "security": "basic_sc",
    "properties": {
        ...
    },
    "actions": {
        ...
    },
    "events": {
        ...
    }
}
```

Fig. 1. Thing Description (TD) document

provides a secure and verifiable means of identity verification. Furthermore, it empowers individuals to selectively disclose only the necessary information, preserving privacy while ensuring trust and security. Considering the huge number of attacks aimed at sniffing data at edge devices, viewing them as a point of failure; decentralized authentication can be used to improve overall security. In this work, we want to extend the use case of SSI to the IoT context, and more in particular to implement a secure authentication framework for the WoT.

The document is structured as follows. The second section discusses existing work related to SSI within the IoT context. The third section introduces the proposed architecture, offering insights on principal components and interactions. The fourth section discusses the findings and results of the proposed solution by considering a specific use case. The last section concludes the work presenting future work and a sum up of relevant points of this work.

II. Background on decentralized authentication within the IoT context

The nodes and users within an IoT ecosystem are assigned a specific digital identity, and, during the authentication, the identity of a requestor has to be validated against specific criteria, so as to let only certain known identities access resources and functions. This is strongly related to authorization, where a specific request is granted to given authenticated entities depending on several factors, such as their role within a given organization or properly formalized security policies. In password-based identity models, such as the one exploited by Kerberos, each entity has a unique identifier and a given password, which are checked by the authenticator so as to validate the identity. Password-based authentication is known to be prone to vulnerabilities and to exhibit a protection degree based on the quality of the used passwords. On the other hand, we have certificate-based identity models, where digital certificates and public-key cryptography are used. X.509 is a standard defining the format of public key certificates and also includes three alternative authentication procedures for a variety of applications. Another solution is provided by Security Assertion Markup Language (SAML), but similarly to X.509, it integrates the authentication logic within the interacting devices. IoT devices have a limit in that they may not hold sufficient computational power and storage capacity to support certificate-based identity and authentication models, while cannot have the various message exchanges underlying such protocols as they can drain a lof of energy and shorten the lifespan of IoT ndoes. Therefore, a token-based approach is being largely adopted. A third-party entity receives the authentication requests containing proper authentication attributes (such as username or password, or even PKI certificates) and issues tokens to be used to be authenticated and request services/data at other IoT devices. This approach has been formalized by JWT or OAuth 2.0 standards [6]. Despite resulting in more lightweight and decoupling the authentication logic from the interacting devices, there is a strong centralization of control, which may lead to security and privacy issues. Moreover, identity management is often siloed by a single authority and does not cope with the multitenant nature of an IoT ecosystem. There is a need to avoid such a centralization while keeping authentication suitable for the key needs of an IoT ecosystem and move away from a siloed identity provider by decentralizing it thanks to a Web 3.0 approach. Such a novel perspective is called decentralised authentication.

Decentralized authentication is a relatively recent field that emerged thanks to the proliferation of blockchains, smart contracts, and dapps, and it paving the way for a moder identity management and authentication. Within the IoT context [7], this owner-centric approach could change the relationships between devices and users allowing multiple benefits for both parties. Fan et al. [8] proposed a framework for integrating decentralized identity management within the IoT context by leveraging blockchain solutions. The authors demonstrate how this technique may be simply implemented to existing technologies by leveraging Amazon Web Services and MQTT. Fedrecheski et al. [9] studied the benefits of decentralized authentication, outlining, among other things, end-to-end security and layered authentication; always regarded as crucial tasks in a dense setting such as the IoT one.

Gebresilassie et al. [10] presented a work that considered SSI as a means for authenticating IoT devices using blockchain-based technologies such as Hyperledger Indy and Distributed Ledger Technologies (DLT). The combination is able to create a strong authentication protocol, where the DLT acts as a shared registry among the network, while Indy wallets are used to securely store the credentials within the device. Standardization of credentials and W3C recommendations have been taken into consideration by De Diego et al. [11], who propose a fully decentralized identity management for the IoT-as-a-service business model. Results confirm the extensibility of the SSI architecture to the IoT context with a validation performed over a Raspberry PI microcontroller. Manoj et al. [12] presented a similar approach applied to the context of smart agriculture. From the study conducted over a large population, it is possible to outline a linear incremental latency in operations executed via the DLT, indicating that this technique is not ideal for the dense IoT context. As

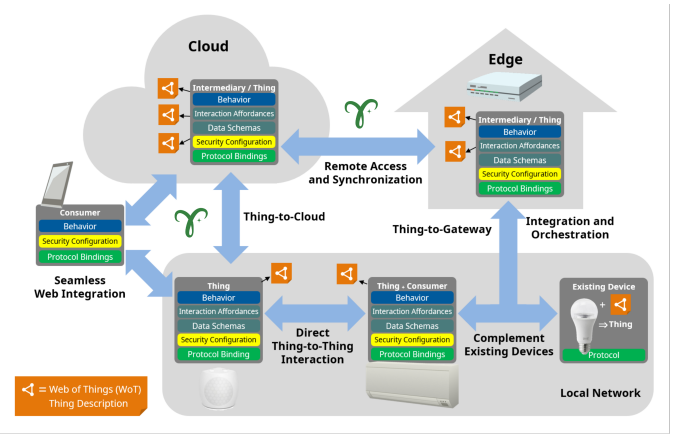

Fig. 2. WoT Architecture [2] with SSI Integration

a consequence, although blockchain-based techniques allow entities to stay more anonymous while guaranteeing revocation at any time, there are some negatives to consider. [13].

The performances of proposed approaches are based on the one of chosen DLT, which usually requires additional overhead to complete operations and may be too much for IoT nodes, opening a room for JSON-LD [14] credentials; known to be more interoperable than Indy-based ones, as they do not need a schema or credential definition to issue credentials [15].

III. Integrating SSI in WoT

The Thing Description (TD) document provides all the necessary information for the interaction with the smart device and is used to handle identification in the context of the WoT architecture (Fig. 2). This identification is usually performed using weak authentication systems based on passwords or centralized servers. The usage of these mechanisms in combination with unsecured channels can lead to sniffing and tampering attacks, as reported in Section 10 of [3].

To prevent these attacks and enhance the security of WoT, the decentralized approach from SSI has to be incorporated into the current architecture. The use of well-established frameworks, such as Hyperledger Aries, allows the design of a secure channel capable of preventing the aforementioned threats. Figure 2 depicts the modified system according to WoT architecture [2], where communication between both Edge and Things must be secured using the proposed protocol. To better explain the integration of SSI within the WoT architecture, we will first explain the structure of JSON-LD credentials with the related signing mechanisms, followed by an implementation of these credentials within Hyperledger Aries using an open-source framework capable of securing the channel and reliably exchanging credentials. Finally, the integration of this authentication within the WoT context is discussed.

A. JSON-LD Verifiable Credentials

Multiple strategies implement Self-Sovereign Identity (SSI), some of them including blockchain while some others do not leverage it. VCs contain claims (pieces of information), cryptographic proofs, and metadata, making verification possible without relying on any authority. The usage of blockchain makes these credentials revocable by publishing on a distributed ledger the public-facing information, but increases the complexity of the system making these credentials not usable within the IoT context due to power and memory requirements.

JSON-LD Credentials, or more properly, Linked Data Proof Veriable Credentials (LDP-VCs) can be held and presented by anyone, independently from the ownership. If someone owns an LDP-VC and loses or unwarranted exchange data with an untrusted party, it will lose the ownership. In addition, LDP-VCs cryptography is less complex than Camenisch-Lysyanskaya (CL) signatures used by AnonCreds. Rivest-Shamir-Adleman (RSA) keys, which are necessary for CL signatures but are huge and possibly slow in limited situations like the Internet of Things (IoT). Lighter signatures such as Ed25519Signature2020 and BbsBlsSignature2020 (BBS+) can be used for signing LDP-VCs. The last one is preferred to the other since provides a multi-message digital signature, meaning that it is possible to split a message signed with a private key into smaller attributes to be shared and verified. While BBS+ permits selective disclosure, JSON-LD aids in controlling the schemas of the data contained within the credential, generating reliable, secure, and well-formed credentials. The creation and exchange of credentials are up to the implementing libraries, responsible for protecting communication and preventing attacks.

B. ACA-Py Framework

ACA-Py is a framework for developing VCs; it uses DIDComm and Hyperledger Aries protocols for establishing trust between parties and securely creating and exchanging VCs. DIDComm is based on the DIDDoc, which is a document containing all the information needed for the communication, like id, set of public keys for the verification, set of authentication methods, and endpoint for the interaction. The strength of this framework is the possibility of executing it over an insecure channel. ACA-Py implements the concept of session DIDs that make possible secure communication creating a DID that does not expose the identity of devices and at the same time is used for ciphering the communication. As depicted in Figure 3, the communication begins with one of two parties that create the invitation (typically the Issuer), containing all the information of DIDDoc. After reading the DIDDoc, the Holder accepts the invitation and HL Aries is responsible for creating a handshake between the two parties in order to create an asymmetric-based encrypted channel. In this exchange, the two parties agree on a session key that must be used, so that there is no possibility for the attacker to steal sensitive information.

Once the secure channel has been established, it is possible to create and exchange verifiable credentials. The enrollment phase, which is executed when a new device wants its own identity, starts with the Issuer that sends JSON-LD Credentials to the Holder by signing it using the BBS+ algorithm. At this

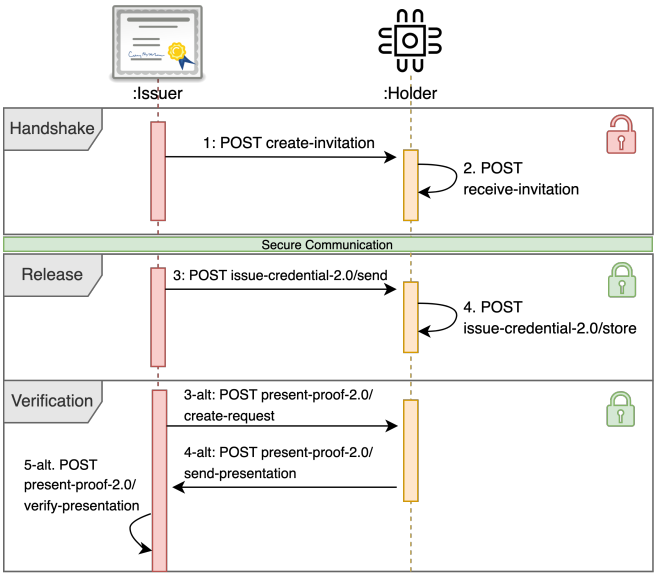

Fig. 3. Sequence diagram of ACA-Py Framework used for credentials exchange

point, the Holder can reject or accept the credential and save it in the Indy wallet.

Once the Holder saves the credentials, can use them for future interactions. The presentation and verification phase starts with a Verifier who sends a presentation request containing a challenge field needed for preventing eavesdropping. In this way, if an attacker captures the packets, it will not be able to use them for future interactions. The Holder will search for the requested credentials, and if at least one of its credentials matches the request, then answer with a presentation. The Verifier must verify the content of the presentation by decrypting the credential sent from the Holder using the public key of the Issuer, contained in the credential.

Differently from blockchain-based SSI, there is no distributed ledger adopted for verifying the identity of the releasing authority or for establishing the validity of sent credentials.

C. Integration within WoT

As introduced in Fig. 1, the TD document is a JSON-based document that contains an attribute for defining the security that must be used for communication. Considering the protocol used by ACA-Py it is possible to extend this document to the needed properties. We can assume that IoT devices store private keys needed for encryption in a secure and tamper-proof memory, which is the Indy wallet. DIDComm leverages a DIDDoc which is a public document containing all the information needed to the protocol for establishing a secure communication and assessing the identity of a device. Such a document is a JSON text with properties like id, set of public keys for the verification, set of authentication methods, and endpoint for the interaction.

It is reasonable to publish the reference to the DIDDoc inside the document as reported from the following code:

```
"security": "ssi",
"securityDefinitions": {
    "ssi": {
        "schema": "didcomm",
        "did": "did:example:123"
    }
}
```

Once resolved the reference to the document it is possible to establish a secure connection with the device and obtain data necessary for the verification of the identity of the IoT edge device. VCs related to the identity of the device will be queried and verified using the ACA-Py framework, as described in the previous subsection.

IV. Results

According to previous work in the literature, the suggested technique was evaluated using three operations: VCs creation, credential exchange, and credential verification.

A. Setup

For evaluating the system, a Raspberry PI 4 Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8GHz processor with 4GB LPDDR4-3200 SDRAM has been used, considering it as the holder. Instead, the issuer and verifier have been run on the same system, an iMac with a 3.33 GHz Intel Core i5 6 core processor and 16 GB 2667 MHz DDR4 RAM.

ACA-Py agents have been deployed on both sides; in particular, the Raspberry Pi uses the Python version of the agent with a manual deployment of needed libraries. Instead, taking into account the resources, the other party has been equipped with a Docker image of the agent.

B. Analysis

Performance analysis has been performed taking into consideration a previous work by De Deigo et al. [11] which evaluated the same operations using a Raspberry PI and ACA-Py agents. The delay introduced by the network can be considered as not relevant since the ping command needs about 5ms to be received and only depends on the quality of the network. Previous work did not consider the connection time, which in our case is relevant for securing the connection. The connection time typically requires less than a minute, with an average of 750ms from the request of connection received. At this time, the two parties agreed on a session DID starting from the information defined in the invitation request.

We took the average of the 1000 requests for credential issues and verification in order to validate the results. Results are provided in Table I and emphasize how the suggested strategy outperforms the memory consumption of the system proposed in [11] for exchange and verification, thanks to various aspects. As stated in the beginning, the purpose of this paper is to offer a secure decentralized system that uses JSON-LD credentials and a BBS+ signature. This type of signing can preserve memory consumption because it doesn't call for CL signatures. Second, rather than leveraging blockchain for identity verification, our credentials only use digital signatures

TABLE I
EXPERIMENTAL RESULTS

Operation	Measure	[11]	Our Approach
VCs Creation	Average	31.07ms	180.48ms
	Std Deviation	4.80ms	14.10ms
Credential Exchange	Average	811.95ms	719.45ms
	Std Deviation	73.69ms	60.63ms
	Avg. CPU Usage	18%	8%
	Avg. RAM Usage	150MB	39MB
Credential Verification	Average	923.92ms	135.61ms
	Std Deviation	44.46ms	16.49ms
	Avg. CPU Usage	19%	10%
	Avg. RAM Usage	150MB	36MB

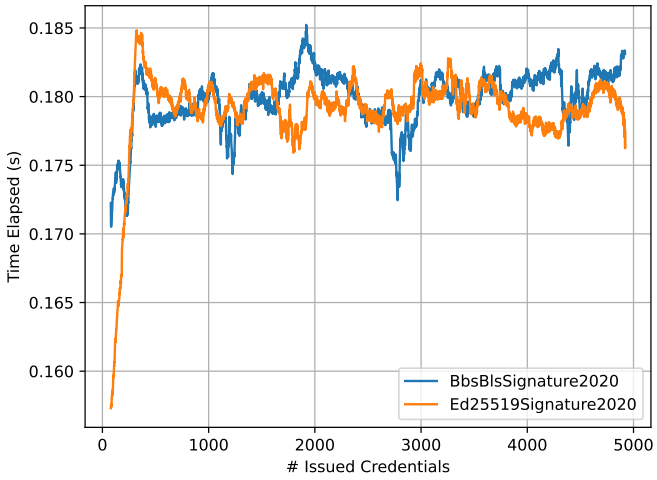

Fig. 4. Number of issued credentials vs. time elapsed for the creation of BBS+ (BbsBlsSignature2020) and Ed25519Signature2020 based credentials.

for credential validation, which reduces the overall time for the verification.

Results suggest that the current approach can be easily implemented in constrained devices, characterized by low memory and processor resources. Despite BBS+ can be considered a lightweight protocol, the time needed for the creation of a credential is higher than the approach based on CL. VCs creation is the only operation that requires more time with respect to [11], but this can be acceptable if considering that the creation is a task that is executed only once for each device.

Figure 4, which illustrates the scalability of the existing technique over 5000 released credentials using BBS+ and Ed25519, shows a non-significant upward trend in the time required to create credentials. The suggested system does not use DLT for registering credentials, in contrast to [12], preventing an exponential rise in the amount of time required. Both the considered algorithms perform creation in a similar time over the number of credentials released, making BBS+ the preferred one considering the selective disclosure capability.

V. CONCLUSION

Privacy and Security in the IoT context are requirements that should be considered in the primary phases of developing a new product, enabling the so-called "privacy-by-default" paradigm. Existing constraints of IoT devices make the creation of authentication algorithms a big challenge. The usage of JSON-LD credentials, in combination with the BBS+ signature is a lightweight solution for extending the SSI architecture to the WoT context. Results show a reduced space for the entire exchange, 39MB and 36MB for issuance and verification respectively; making these credentials suitable for constrained devices. However, revocation of these credentials remains difficult if a distributed ledger is not used, as in the case of Indy-based credentials.

ACKNOWLEDGEMENTS

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

REFERENCES

[1] A. Khurshid, R. Alsaaidi, M. Aslam, and S. Raza, "Eu cybersecurity act and iot certification: Landscape, perspective and a proposed template scheme," *IEEE Access*, vol. 10, pp. 129 932–129 948, 2022.

[2] M. Kovatsch, R. Matsukura, M. Lagally, T. Kawaguchi, K. Toumura, and K. Kajimoto. (2023) Web of things (wot) architecture 1.1. [Online]. Available: https://www.w3.org/TR/wot-architecture11/

[3] S. Kaebisch, M. McCool, E. Korkan, T. Kamiya, V. Charpenay, and M. Kovatsch. (2023) Web of things (wot) thing description 1.1. [Online]. Available: https://www.w3.org/TR/wot-thing-description11/

[4] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[5] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of iot security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, p. 100585, 2023.

[6] P. Solapurkar, "Building secure healthcare services using oauth 2.0 and json web token in iot cloud scenario," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 2016, pp. 99–104.

[7] R. P. Sukumaran and S. Benedict, "Survey on blockchain enabled authentication for industrial internet of things," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 1510–1516.

[8] X. Fan, Q. Chai, L. Xu, and D. Guo, "Diam-iot: A decentralized identity and access management framework for internet of things," in *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 2020, pp. 186–191.

[9] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, and M. K. Zuffo, "Self-sovereign identity for iot environments: A perspective," in *2020 Global Internet of Things Summit (GIoTS)*, 2020, pp. 1–6.

[10] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui, "Distributed, secure, self-sovereign identity for iot devices," in *2020 IEEE 6th World Forum on Internet of Things*, 2020, pp. 1–6.

[11] S. De Diego, C. Regueiro, and G. Macia-Fernandez, "Enabling identity for the iot-as-a-service business model," *IEEE Access*, vol. 9, pp. 159 965–159 975, 2021.

[12] T. Manoj, K. Makkithaya, and V. Narendra, "A trusted iot data sharing and secure oracle based access for agricultural production risk management," *Computers and Electronics in Agriculture*, vol. 204, p. 107544, 2023.

[13] S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, "Blockchain-based decentralized identification in iot: An overview of existing frameworks and their limitations," *Electronics*, vol. 12, no. 6, p. 1283, 2023.

[14] M. Sporny, D. Longley, G. Kellogg, M. Lanthaler, and N. Lindström, "Json-ld 1.1," *W3C Recommendation, Jul*, 2020.

[15] K. Young, "Verifiable credentials flavors explained," *Linux Foundation Public Health: Linux Foundation Public Health*, 2021.