Verifiable Credentials and BBS＋ Signatures

2.1 Introduction

The concept of self-sovereign identity (SSI) is drawing attention as a new type of digital identity. A digital identity represents who you are in digital space and consists of a collection of attributes such as name, date of birth, gender, and email address[*1]. Digital identities have traditionally been managed by applications, enterprise systems, or identity providers such as GAFAM. The idea of SSI is to allow the owner of an identity to independently manage the identity.

Two years have passed since we discussed SSI in IIR Vol. 43[*2]. Over that time, the technologies and mechanisms needed to make SSI a reality have continued to advance; this includes Verifiable Credentials (VC), Decentralized Identifiers (DIDs), digital agents, digital wallets, and governance frameworks. These technologies are comprehensively explained in other documents[*3][*4], and here we limit our focus to providing an overview of VCs, which can be considered the core of SSI. We also briefly discuss the implementation of VCs using BBS＋ signatures, which have been attracting interest in the community since last year.

2.2 Credentials and Verifiable Credentials

The term "credentials" can mean various things depending on context[*5], but here we refer to the World Wide Web Consortium (W3C) specification[*6] and use the term to mean "a set of one or more claims about a subject made by an issuer". For example, a driver's license is a type of credential in that it is a set of claims (e.g., the holder's name, address, date of birth, photograph, types of vehicles that can be driven) that the issuer (e.g., department of motor vehicles) makes about the subject (i.e., the license holder).

Credentials allow us to have the credential issuer vouch for who we are. For example, if I were trying to open a bank account, the bank teller would not trust me if I simply claimed, without any evidence, that "I am a male living in ABC City and my birthdate is XYZ". Showing my driver license, which serves as my credentials, in this case means that the license issuer certifies my claims, and this enhances the credibility of my claims[*7].

For a claim made using credentials to be accepted, however, the credentials must be credible to the party to which the claim is made. So who issued the credentials? Have the credentials been rewritten or forged by someone else? Have they expired or been revoked? Only once these things are verified and validated can the information in the credentials be accepted.

With physical credentials, the verifier looks at the information on the document and determines its authenticity by checking any special printing, such as watermarks, if present. This sort of verification process is often difficult and requires specialized skill.

VCs are digitalized credentials, so they can be verified by a computer. This does not mean that the credentials document is simply scanned into a digital image. Digital signatures are used to verify the issuer's identity and whether or not the document has been tampered with. This approach is based on the results of cryptographic research into what's known as anonymous credentials or attribute-based credentials, and it can also accommodate privacy-enhancing mechanisms using zero-knowledge proof technology.

*1 ISO/IEC 24760-1 defines identity as "a set of attributes related to an entity".

*2 Internet Infrastructure Review Vol. 43, "2. Blockchain-based Identity Management and Distribution" (https://www.iij.ad.jp/en/dev/iir/043.html).

*3 Alex Preukschat and Drummond Reed, "Self-Sovereign Identity - Decentralized digital identity and verifiable credentials", Manning Publications, May 2021 (https://www.manning.com/books/self-sovereign-identity).

*4 Kengo Suzuki and Kento Goro, "Identity wa dare no mono? Hyperledger Indy & Aries de jitsugen suru bunsan identity" [Who do identities belong to? Decentralized identities made possible by Hyperledger Indy & Aries] Impress R&D, May 2021, (https://nextpublishing.jp/isbn/9784844379447, in Japanese).

*5 Internet Infrastructure Review Vol. 26 "1.4.3 ID Management Technology" (https://www.iij.ad.jp/en/dev/iir/026.html).

*6 Verifiable Credentials Data Model 1.0 (https://www.w3.org/TR/vc-data-model).

*7 A driver's license is first and foremost a credential to show that you are qualified to drive. Driver's licenses are also commonly used as a form of ID since they contain a set of key attributes, such as name, address, gender, date of birth, and face photo. The government has also identified integrating driver's licenses with Japan's Individual Number Cards as a goal.

2.3 Illustration of Verifiable Credentials in Use

To provide a more tangible idea of how VCs are used, let's imagine a world in which certificate of residence (a common identification document in Japan) are represented as VCs and consider what happens from issuance through to the use of these credentials.

Mr. A, who lives in X City, decides to sign up for a family account on a service provided by Company B. Company B offers a discount to residents of X City. To receive the discount, Mr. A needs to show that he and his family live in X City.

So Mr. A visits the X City residential services office and asks for a VC version of his certificate of residence.

X City residential services verify Mr. A's identity using an appropriate method. They may, for example, ask him to present a photo ID in person or to provide other VCs online.

Upon confirming Mr. A's identity, X City residential services obtain the attributes of Mr. A and his family from the resident information database and issue a VC, which is equivalent to a certificate of residence and contains the attributes of Mr. A and family, including address, name, date of birth, gender, and date resident status was obtained. Mr. A stores the VC in his smartphone.

Mr. A then applies to Company B for the service. By presenting the VC issued by X City to Company B, Mr. A can show that he and his family reside in X City.

Both Mr. A and Company B want to exchange only a minimum of personal information. So, Mr. A presents the credentials to Company B with only the address of Mr. A and family disclosed (i.e., selective disclosure) and the rest of the information hidden (name, gender, date of birth, and date of residential status). Figure 1 illustrates this. In this example, we assume that Company B has specified what attributes it needs (address), but it is also possible for Mr. A to choose which attributes are provided.

Company B verifies the credentials and confirms that Mr. A and his family reside in X City, as asserted by X City. This allows Mr. A and his family to use Company B's service at a discounted price.

Note that the VC Mr. A received from X City is not specific to Company B's services. For example, Mr. A can subsequently show some other company—call it Company C—that he lives in X City or perhaps that members of his family are over 20 years old. It is also envisioned that, in addition to using a single VC, people will be able to combine multiple VCs to provide the desired attributes.

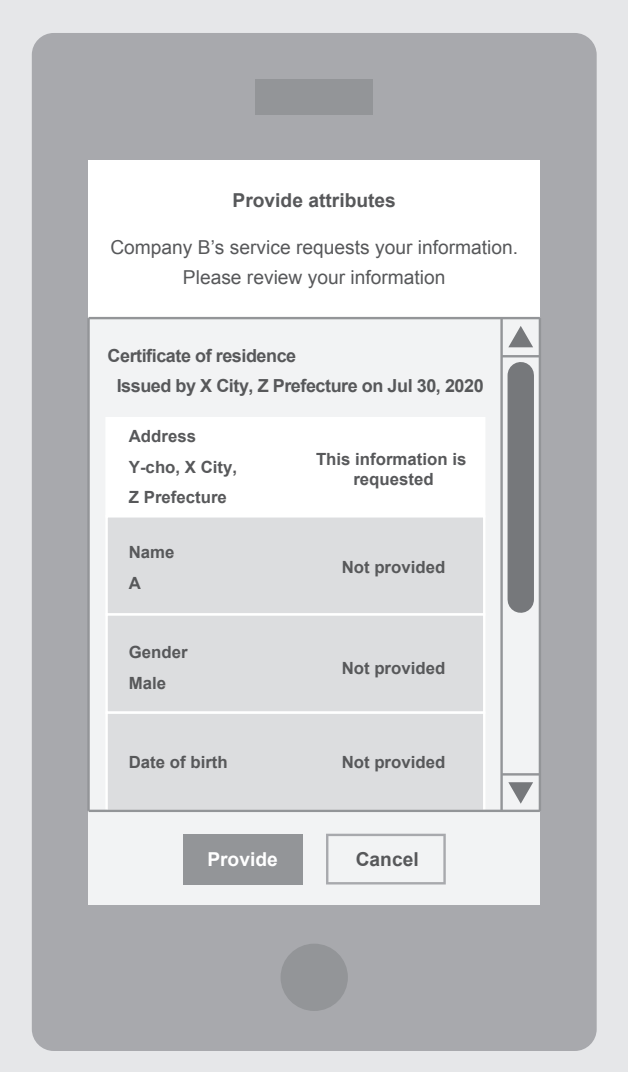

Figure 1: Illustration of Providing Credentials

2.4 The Verifiable Credentials Ecosystem

In the example above, we encountered X City, which issued the VC, Mr. A, who received the VC and presented it to another party, and Company B, which verified the credentials presented. The actors in a VC scenario and the relationships between them are called the Verifiable Credentials ecosystem, which can be laid out as in Figure 2.

The issuer is the person or organization that issues the VC. In the previous example, this is X City.

The holder receives the VC issued by the issuer and stores it in his/her smartphone or other device. The holder then presents the VC to verifiers as needed. In the example above, Mr. A was the holder of a VC version of his certificate of residence.

The subject is an entity about which the VC makes claims. In most cases, the subject is the same as the holder, but they can be different entities in some cases, such as when the subject is an infant and the holder is the infant's guardian. In the example above, the subject encompasses Mr. A as well as his family members.

The verifier is the person or organization that verifies the VC presented by the holder and uses the information it contains. In the example above, this is Company B and Company C.

The Verifiable Data Registry is data storage used by the issuers, holders, and verifiers. It records information required for performing verification, such as the issuer's identifier and public key and credential revocation registries. Anyone can refer to this information, but it cannot be altered. As such, it is often implemented on a blockchain.

VCs and self-sovereign identity are often mentioned in conjunction with blockchain, and it is common to think that VC itself is recorded on a blockchain, but this is a misconception. The Verifiable Data registry is a registry that anyone can refer but not alter, so it is not considered an appropriate place for VCs containing personal data[*8].

As the previous example illustrates, the two major VC events occur when the issuer issues credentials and when the holder presents them to a verifier. The holder asks the issuer to issue credentials and is thus issued with a VC that contains the subject's attributes. The holder saves this on her smartphone or other device and later presents only the necessary parts to verifiers, who then verify the credentials. The result is that the verifier is able to confirm that the subject has the attributes as certified by the issuer.

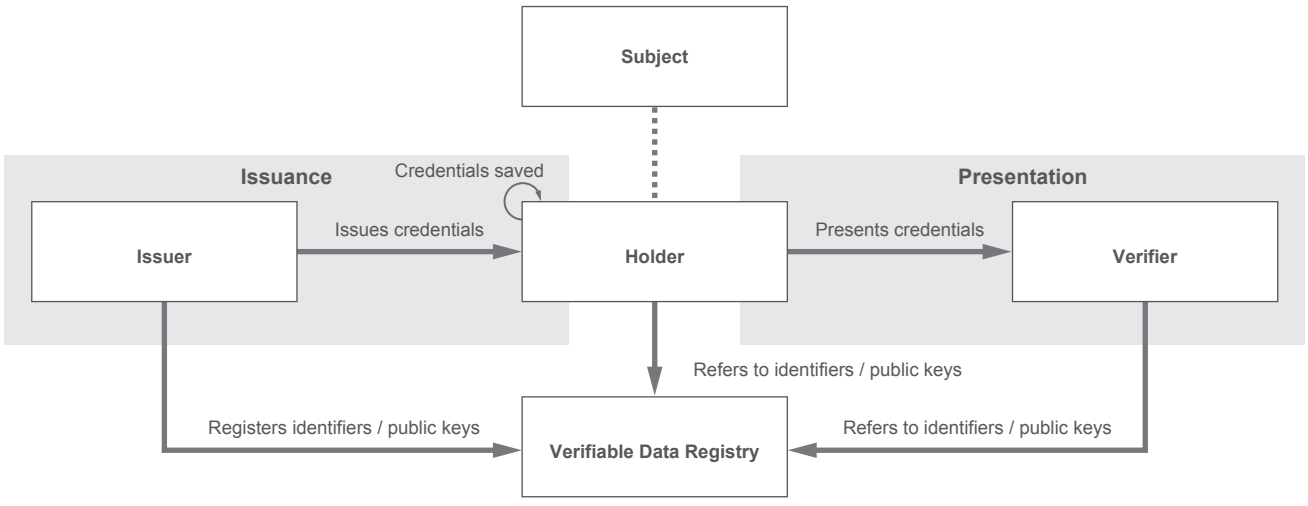

Figure 2: Verifiable Credentials Ecosystem

*8 Stephen Curran, "Why Distributed Ledger Technology (DLT) for Identity?", Hyperledger (https://www.hyperledger.org/blog/2021/04/21/why-distributed-ledger-technology-dlt-for-identity).

2.5 How Verifiable Credentials and Traditional Digital Certificates Differ

Credentials that use digital signatures are actually not a new concept. Digital certificates are constantly being verified when we communicate via HTTPS on a daily basis. OpenID Connect, which is often used for digital identity federation, also stores identity information in digitally signed ID tokens to facilitate verification. In that sense, these digital certificates and tokens also serve as verifiable credentials.

So how do VCs and traditional digital certificates differ? We see three main points. Not all VCs check all of these points, but we seem to call credentials VCs when at least one of these characteristics is present.

1. Has a mechanism for providing only the minimum of data required
2. A holder is always present between the issuer and the verifier
3. Uses a decentralized identifier (DID)

Let's start with the first point. Many VCs have a mechanism for minimizing the data that the credential holder discloses. One of the most notable is the use of a cryptographic technique called zero-knowledge proofs. A zero-knowledge proof allows the holder to present only the attributes in credential that the verifier requires while keeping other attributes hidden. It is also possible to disclose only the fact that the hidden attributes satisfy certain conditions. For example, the holder can hide the name, address, and date of birth on a driver's license while also showing that he is qualified to drive a standard automobile and that he is at least 20 years of age. This sort of mechanism is key to protecting the privacy of the holder and subject.

The second point also has to do with protecting the holder's privacy. If we consider the issuer to be the Identity Provider (IdP) and the verifier to be the Relying Party (RP), then the VC mechanism can be seen as similar to existing identity federation mechanisms such as OpenID Connect and SAML. VCs differ from these standards in that they do not allow direct interaction between the issuer and the verifier; there is always a holder between the two. This aspect of VCs is one reason they play a central role in SSI. It is useful because the holder may not want the issuer and verifiers to know his every move in terms of what information he has provided to what sort of providers and when.

The third point relates to decentralized identifiers (DIDs), which, along with VCs, are the cornerstone of SSI. DIDs are identifiers that can refer to people, organizations, and things, and they are associated with a public key that is needed to verify the digital signature. The association between the DID and the public key is guaranteed in a decentralized manner using blockchain or the like without the need for a trusted third party such as a registration authority. One does not need to use DIDs to realize the benefits of VCs, but they are often used together to unlock the advantages of both in tandem.

2.6 Developments in Verifiable Credentials

Vaccination certificate implementations that use these characteristics of VCs and other initiatives are being trialled.

In April 2020, the COVID-19 Credentials Initiative (CCI) was launched to enable the application of VCs to facilitate the interoperable use of privacy-preserving digital credentials for COVID-19-related purposes[*9]. The CCI has now joined Linux Foundation Public Health (LFPH)[*10]. In June 2021, LFPH launched the Global COVID Certificate Network (GCCN), a cross-border initiative for the exchange of vaccination certificates[*11]. Meanwhile, in January 2021, Microsoft, Oracle, Salesforce, and others also launched the COVID-19 Credentials Initiative (CCI), which is working to digitalized vaccine certificates based on VCs[*12].

Similarly, the European Digital Identity Framework unveiled by the European Commission in June 2021 put forward the concept of a Digital Identity Wallet usable by all citizens and residents of EU member states. Although it does not specifically mention the use of VCs and SSI, the heavy influence of VCs is apparent given that the model and use cases comprise issuers, holders, and verifiers and that holders can selectively disclose attributes[*13].

The use of VCs is also expanding to include other areas, with examples being eKYC (online know your customer) for microfinance by the NPO Kiva[*14] and the IATA Travel Pass[*15] from the International Air Transport Association (IATA).

In Japan, Keio University, together with five Japanese companies and in cooperation with Microsoft, commenced demonstration testing of student identity system that uses VCs and DIDs in October 2020[*16]. And in a March 2021 white paper, the Trusted Web Promotion Council mentions VCs as one of the building blocks for realizing trustable communication[*17].

A slew of products supporting such use cases is being developed. The Linux Foundation's Hyperledger project is heavily engaged in developing a range of technologies, with a particular focus on Hyperledger Indy[*18], a distributed ledger for providing DIDs, Hyperledger Aries[*19], an agent for handling VCs, and Hyperledger Ursa[*20], a cryptographic library for use by these projects. Azure AD, Microsoft's Identity as a Service (IDaaS) offering, also includes VC functionality and has been in public preview since April 2021[*21].

*9 CCI (COVID-19 Credentials Initiative) (https://www.covidcreds.org/).

*10 LFPH (Linux Foundation Public Health) (https://www.lfph.io/).

*11 Introducing the Global COVID Certificate Network (GCCN) (https://www.lfph.io/2021/06/08/gccn/).

*12 Vaccination Credential Initiative (VCI) (https://vaccinationcredential.org/).

*13 European Digital Identity - European Commission (https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en).

*14 Kiva Protocol, built on Hyperledger Indy, Ursa and Aries. Sierra Leone has adopted this protocol and built a platform that allows people perform identity verification in around 11 seconds for the purpose of small-scale financing. (https://www.hyperledger.org/blog/2021/01/20/kiva-protocol-built-on-hyperledger-indy-ursa-and-aries-powers-africas-first-decentralized-national-id-system).

*15 IATA - Travel Pass Initiative (https://www.iata.org/en/programs/passenger/travel-pass/).

*16 "Keio University Commences Demonstration Experiment of Next-Generation Digital Identity Platform: To Issue Certificates of Enrollment and Certificates of Expected Graduation to Smartphone Applications" (https://www.keio.ac.jp/en/press-releases/2020/Nov/13/49-76286/).

*17 Trusted Web White Paper ver 1.0 (https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/documents_210331-2.pdf, in Japanese).

*18 Hyperledger Indy (https://www.hyperledger.org/use/hyperledger-indy).

*19 Hyperledger Aries (https://www.hyperledger.org/use/aries).

*20 Hyperledger Ursa (https://www.hyperledger.org/use/ursa).

*21 Identity verification solutions - Microsoft Security (https://www.microsoft.com/en-us/security/business/identity-access-management/verifiable-credentials).

2.7 Verifiable Credentials Implementations

While W3C is working to standardize VCs, this standardization effort is focused on the data model. Specific details vary widely from implementation to implementation. An explanatory document[*22] by CCI and LFPH refers to these variations in implementation as “flavors”.

Here, we look at JSON-LD ZKP with BBS+, a flavor that has attracted a lot of attention at the Internet Identity Workshop (IIW)[*23] and in related circles. JSON-LD ZKP with BBS+ is a relatively new scheme that was unveiled by New Zealand-based company MATTR at the April 2020 IIW. It has been well received by the community[*24], and non-MATTR engineers are now also involved in developing and discussing the scheme’s standard as part of the W3C Credentials Community Group (CCG)[*25] and the Decentralized Identity Foundation’s (DIF) Crypto Working Group[*26]. It is being developed in the open on GitHub[*27], where we have also made a few contributions.

Key aspects of JSON-LD ZKP with BBS+ are that it uses the JSON-LD format to encode credentials, and it uses BBS+ signatures, which work well with zero-knowledge proofs, as the digital signature scheme.

The JSON-LD specification is not as well known as JWTs (JSON Web Tokens) in a digital identity context, but it is widely used in the Semantic Web and Search Engine Optimization (SEO) domains. An advantage of JSON-LD is that it incorporates Linked Data elements into JSON data and can thereby uniquely identify the terms used to describe data using URIs while retaining the compactness of JSON. Metadata in JSON-LD format is embedded in many websites these days. Figure 3 shows an example of a credential represented in JSON-LD.

BBS+ signatures are multi-message digital signatures[*28][*29][*30] that extend BBS group signatures[*31]. They are a type of elliptic curve cryptography that uses an operation called

```
{
    "@context": [                           // JSON-LD context
        "https://www.w3.org/2018/credentials/v1",
        "https://schema.org",
        ...
    ],
    "id": "http://example.edu/creds/1234",      // Credential identifier
    "type": "VerifiableCredential",             // Credential type
    "issuer": "https://example.edu/issuers/1",  // Credential issuer
    "issuanceDate": "2021-06-22T00:00:00Z",     // Credential issue date
    "expirationDate": "2022-06-22T00:00:00Z",   // Credential expiry date
    "credentialSubject": {
        "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  // Subject identifier
        "type": "Person",                               // Subject type
        "birthDate": "1970-01-01",                      // Subject DOB
        "name": "John Smith",                           // Subject name
        ...                                             // Other attributes
    },
    "proof": { ... }                        // Signature value needed for verification etc.
}
```

Figure 3: Example of JSON-LD Credentials

*22 A Path Towards Interoperability: CCI Released a Paper on Different Flavors of Verifiable Credentials (https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/).
*23 Internet Identity Workshop (https://internetidentityworkshop.com/).
*24 Why the Verifiable Credentials Community Should Converge on BBS+ (https://www.evernym.com/blog/bbs-verifiable-credentials/).
*25 BBS+ Signatures 2020, W3C Community Group Draft Report (https://w3c-ccg.github.io/ldp-bbs2020/).
*26 DIF - Applied Crypto Working Group (https://identity.foundation/working-groups/crypto.html).
*27 mattrglobal/jsonld-signatures-bbs: A linked data proof suite for BBS+ signatures (https://github.com/mattrglobal/jsonld-signatures-bbs/).
*28 Jan Camenisch and Anna Lysyanskaya, “Signature Schemes and Anonymous Credentials from Bilinear Maps”, CRYPTO 2004 (http://dx.doi.org/10.1007/978-3-540-28628-8_4).
*29 Man Ho Au, Willy Susilo, and Yi Mu, “Constant-Size Dynamic k-TAA”, SCN 2006 (http://dx.doi.org/10.1007/11832072_8).
*30 Jan Camenisch, Manu Drijvers, and Anja Lehmann, “Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited”, Trust 2016 (http://dx.doi.org/10.1007/978-3-319-45572-3_1).
*31 Dan Boneh, Xavier Boyen, and Hovav Shacham, “Short Group Signatures”, CRYPTO 2004 (http://dx.doi.org/10.1007/978-3-540-28628-8_3).

pairing. They differ from the commonly used RSA and ECDSA signatures in that it is possible to sign a list of multiple pieces of data (rather than a single piece of data). The structure also makes it easy to combine with zero-knowledge proof technology, so you can verify a signature as being valid while still hiding some elements in the list of signed data, and you can hide selected elements while still providing proof that they meet some criteria.

JSON-LD ZKP with BBS+ canonicalizes credentials represented in JSON-LD into a data form called statements using LD canonicalization. BBS+ signatures are then used to sign and verify the list of statements. For example, the JSON-LD credentials in Figure 3 are converted into a list of statements as shown in Figure 4 and then signed. Using BBS+ signatures to sign the list of statements allows you to control whether each particular statement is shown or not. It is not yet possible, however, to provide high-level proofs showing that a particular value within a statement (name, date of birth, etc.) satisfies certain conditions (e.g., date of birth falls within a certain range) while keeping that value hidden.

2.8 The Future of Verifiable Credentials

Some issues remain to be resolved before VCs and JSON-LD ZKP with BBS+ can be put to practical use. Here, we go over three key issues and look at approaches and efforts aimed at solving them.

■ Issue 1: Interoperability with existing digital identity technologies

The first challenge is ensuring interoperability between the new concept that VCs represent and existing digital identity specifications and products. The OpenID Foundation (OIDF) is looking at addressing this by using the Self-Issued OpenID Provider (SIOP) framework, which is originally part of OpenID Connect, to handle VCs on top of OpenID Connect. Engineers from MATTR, the original proponent of JSON-LD ZKP with BBS+, are involved in this work.

■ Issue 2: Standardizing the various specifications

The JSON-LD ZKP with BBS+ and LD canonicalization specifications mentioned above are still being discussed and not yet finalized as standard specifications. In the case of JSON-LD ZKP with BBS+, the W3C CCG is developing the specification and, in parallel with this, DIF's Crypto Working Group is also holding discussions, as mentioned earlier. The details are being standardized as W3C specifications as they are finalized, with future details to be discussed and worked out by the DIF's Crypto Working Group. For example, the means of making high-level proofs possible, such as showing that a person is 20 years or older while keeping date of birth hidden, is on the DIF Crypto Working Group's agenda for discussion. As for LD canonicalization, the W3C's Linked Data Signatures Working Group currently being set up is expected to pursue work on this in the form

```
<did:example:ebfeb1f712ebc6f1c276e12ec21> <http://schema.org/birthDate> "1970-01-01"^^<http://schema.org/Date> .
<did:example:ebfeb1f712ebc6f1c276e12ec21> <http://schema.org/name> "John Smith" .
<did:example:ebfeb1f712ebc6f1c276e12ec21> <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <http://schema.org/Person> .
<http://example.edu/creds/1234> <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://www.w3.org/2018/credentials#VerifiableCredential> .
<http://example.edu/creds/1234> <https://www.w3.org/2018/credentials#credentialSubject> <did:example:ebfeb1f712ebc6f1c276e12ec21> .
...
```

Figure 4: List of Signed Statements (Excerpt). Each Line is Called a Statement.

of RDF Dataset Canonicalization (RDC) and Linked Data Integrity (LDI). As of this writing (August 2021), the aim according to the Proposed Charter[*32] is to begin work in September 2021 and produce a W3C Recommendation by September 2023, or within two years.

■ Issue 3: Resilience to quantum computing

The third issue to highlight, and a long-term one, is that of post-quantum cryptography, which we also covered back in IIR Vol. 49[*33]. The security of BBS+ signatures relies on the hardness of the discrete logarithm problem on elliptic curves. It is known that quantum computers will be able to efficiently solve this problem. So, unfortunately, BBS+ signatures and JSON-LD ZKP with BBS+, which uses them, are not quantum resistant. The same goes for the Camenisch-Lysyanskaya (CL) signatures used in Hyperledger Indy as well as the RSA, ECDSA, and EdDSA signatures often used in JWTs. Post-quantum anonymous credentials based on lattice-based signature schemes and Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARK) have also been proposed, but much room for improvement, including performance enhancements, remains before they become practically viable.

2.9 Conclusion

We have looked at the current status of and future issues for VCs, a topic that continues to gain attention, and one of the implementations in the form of the JSON-LD ZKP with BBS+ flavor. Personally, I expect VCs to be used as and when appropriate rather than completely replacing conventional digital certificates and ID tokens. The real value of VCs is evident in situations where the privacy of people, organizations, and things must be protected, particularly when there is a need to minimize what data is provided. And VCs that use JSON-LD make possible credential statements with strong expressive power and interoperability, facilitating digital identity bridging across a wide range of organizations and industries. Many issues remain to be resolved before VCs are used in real-world applications, but we will be keeping an eye on efforts to standardize and popularize their use, and we hope to make our own contributions toward the development of the community in this area as well as society as a whole.

Dan Yamamoto
Senior Engineer, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ.
Dr. Yamamoto began his current role in 2021. He investigates and researches digital identity and information security issues.

*32 Linked Data Signatures Working Group Charter (https://w3c.github.io/lds-wg-charter/index.html).
*33 Internet Infrastructure Review Vol. 49, "Trends in Post-Quantum Cryptography—2020" (https://www.iij.ad.jp/en/dev/iir/049.html).