Bank of Japan Review

2026-E-6

Verifiable Credentials for Identity Assurance in the Digital Society: An Overview and Trends in Standards Development

Payment and Settlement Systems Department:

YAMADA Nodoka, SHINZAKI Takashi, SHIMIZU Tomoko, OKABE Kota

April 2026

With the advancement of digitalization, the importance of securely and reliably proving one's identity using digital technologies has been growing. In this context, Verifiable Credentials (VCs) are attracting attention. A VC is a versatile and machine-readable "digital certificate" with functions to ensure authenticity and prevent tampering by using digital signatures. In addition to the use of VCs for COVID-19 vaccination certificates, their utilization is being explored in a wide range of domains, including financial practices. Various organizations have also been advancing standards development for VCs. For example, in October 2024, the International Organization for Standardization (ISO) published the international standard for the verifiable Legal Entity Identifier (vLEI), a type of VC. This report provides an overview of VCs, their use cases, and trends in the development of related standards.

Introduction

As the advancement of digitalization has increased the risks of privacy breaches, impersonation, and data falsification, the importance of securely and reliably proving "who you are" — that is, one's identity — using digital technologies has further increased. At the same time, from the perspective of enhancing convenience across society, a system that enables rapid verification of presented certificates is required.

As a technology that addresses such social needs, Verifiable Credentials (VCs) are attracting attention. By leveraging VCs, individuals and companies can show their attributes —such as information about certificate holders' identities or their qualifications and rights —in a secure and highly reliable manner.

Initiatives for utilizing VCs have begun to progress in various fields. After VCs were used for COVID-19 vaccination certificates, governments, industry organizations, and private companies in various countries, including Japan, are exploring the expansion of their applications. Concurrently, standards development for VCs is underway in various organizations. In October 2024, the International Organization for Standardization (ISO) published the international standard for the verifiable Legal Entity Identifier (vLEI), a type of VC.

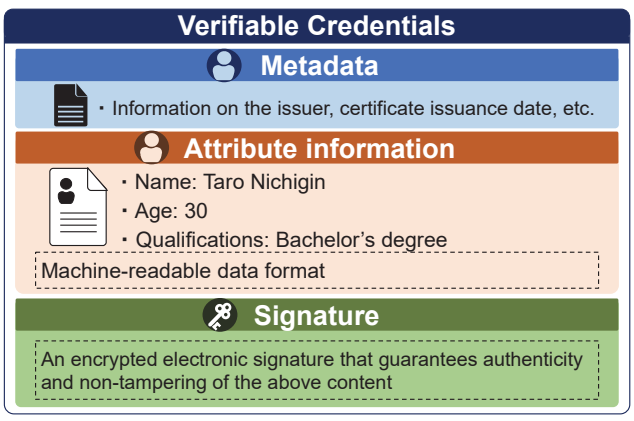
This report provides an overview of VCs and explains their technological features and use cases. It then surveys trends in the development of VC-related standards and presents the vLEI as a specific example.

About VCs

Overview of VCs

A VC [1] is a digital certificate designed with a versatile and machine-readable data format to ensure authenticity and prevent tampering by using digital signatures. Specifically, VCs contain metadata about the issuer and other information, attribute information of the holder, and a digital signature that ensures the authenticity and integrity of the certificate. These elements are expressed in various data formats, such as SD-JWT and mdoc (Figure 1).

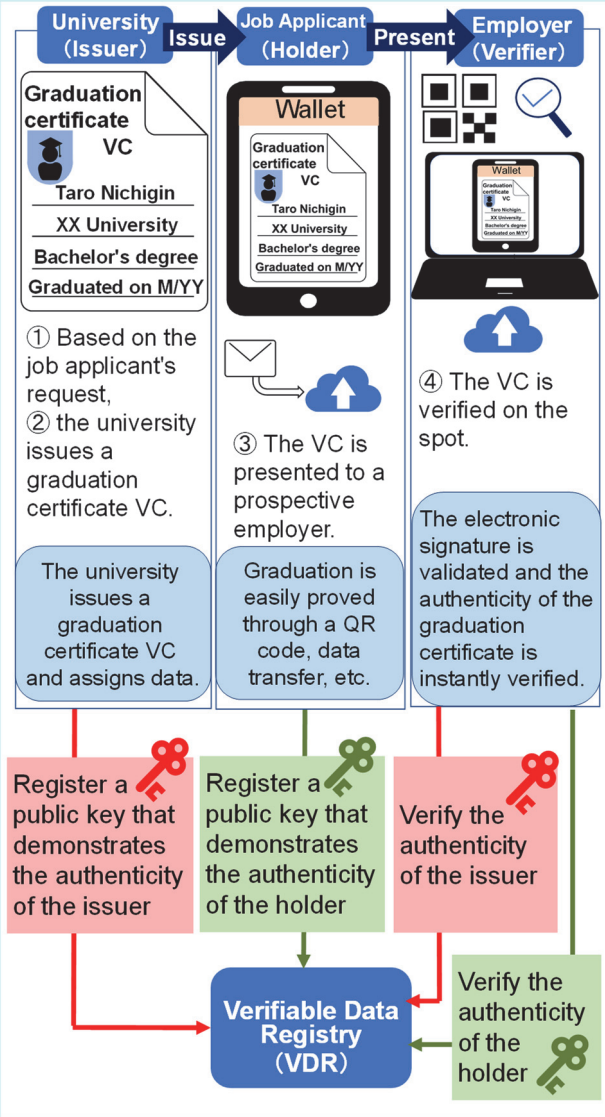
[Figure 1] Structure of VCs



(Note) Prepared by the authors based on the World Wide Web Consortium's (W3C) specifications, etc.

To provide a concrete picture of the use of VCs, consider a case in which a job applicant presents a graduation certificate (VC) issued by a university to a prospective employer. The process is as follows (Figure 2).

[Figure 2] How VCs are used in practice



(Note) Prepared by the authors based on the materials of the Digital Agency and other sources.

First, (i) the job applicant with a university degree requests the university to issue a graduation certificate (VC). Next, (ii) the university (Issuer) issues a VC signed with the university's private key to the job applicant's wallet[2] (an application that receives, stores, and presents VCs). Then, (iii) the job applicant (Holder) signs the VC with their own private key using their wallet and presents the graduation certificate (VC) to the prospective employer. Lastly, (iv) the prospective employer (Verifier) verifies the authenticity of the received graduation certificate (VC), based on the public keys of the university and the job applicant. In this process, the authenticity of the signatures that have been provided by the two private keys is ensured by verifiable data about the holders of the private keys, which have been registered on a Verifiable Data Registry (VDR), such as a blockchain or web server.[3] This is how the authenticity of the graduation certificate (VC) is verified. As this example illustrates, the key feature of VCs is that they enable the exchange of information in a highly convenient manner while ensuring the authenticity of the VC holder's attribute information.

This process is based on the fundamental framework of VCs, known as the "IHV model." The IHV model explains the entire process using VCs through the roles of the three parties - the Issuer, the Holder, and the Verifier - and is named after the initials of the three parties. The Issuer is an entity that issues a VC. The Holder is an entity that manages the issued VC, and the Verifier is an entity that validates the content of the presented VC to verify its authenticity. In the example of receiving, presenting, and verifying a graduation certificate, the Issuer is the university, the Holder is the job applicant, and the Verifier is the prospective employer. The entire process works when these three parties perform their respective roles.[4] VCs based on the IHV model have been implemented for COVID-19 vaccination certificates and mobile driver's licenses in the United States.[5]

Compared with paper-based certificates, utilizing VCs offers various advantages. In the above example, VCs reduce the burden of issuing and obtaining paper-based graduation certificates for both the university (Issuer) and the job applicant (Holder) – such as eliminating the need to request a certificate by mail and reducing the number of days required for obtaining them. For the employer, VCs ensure the authenticity of the certificate, thereby lowering the risk of forgery and enabling faster verification. VCs are expected to significantly improve convenience for issuers, holders, and verifiers while also ensuring the authenticity of certificates.

Technological Features of VCs

One of the technological features of VCs is the flexibility of their data formats. Data formats are defined by various standards to enable the incorporation of diverse attribute information in VCs. In addition, VCs support the selective disclosure of the Holder's diverse attribute information to the Verifier, rather than disclosing all information at once. The ability to protect personal information and enhance

privacy is also a significant feature of VCs[6] (Figure 3).

Furthermore, unlike traditional electronic certificates (ECs), VCs do not necessarily require a centralized database. Verification of attribute information is completed by the Holder presenting their VC and the Verifier verifying its digital signature. Thus, the structure of information management is more decentralized compared with that of traditional electronic certificates, which is another significant feature of VCs.

[Figure 3] Comparison of VCs and traditional Electronic Certificates

Features	Format	Description
Overview	VC	Proves the subject's attributes
	EC	Proves that the subject is the holder of the key
Flexibility of the format	VC	・ Flexible ・ Includes diverse attributes
	EC	・ Inflexible ・ Only handle single attribute
Selective disclosure	VC	Supports selective disclosure
	EC	Does not support selective disclosure
Information management	VC	Does not require a centralized database
	EC	Requires a centralized database
Examples	VC	・ COVID-19 vaccination certificates ・ In the case of VC for a graduation certificate, it ensures the authenticity of the certificate.
	EC	・ Signature of Individual Number Card ・ In the case of VC for a graduation certificate, it only ensures the authenticity of the university's public key.

(Note) Prepared by the authors based on various materials.

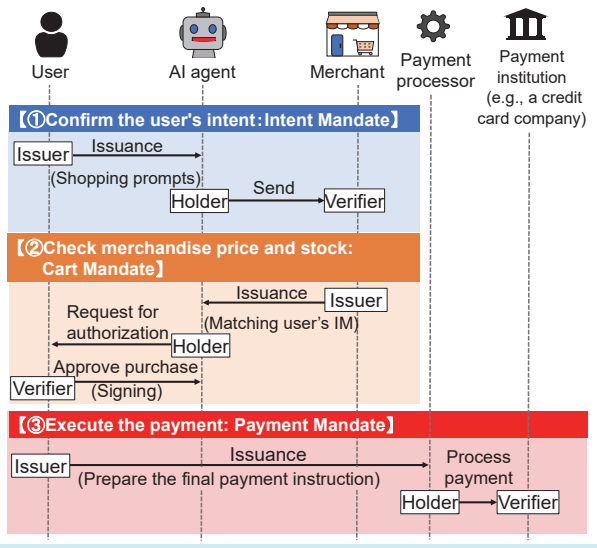
Use Cases of VCs

As stated above, the practical development of VCs is already underway, including COVID-19 vaccination certificates and mobile driver's licenses in the United States. The following two examples illustrate potential future applications.

The first is a scheme being considered in Japan by the Decentralized Identifier/Verifiable Credential Co-Creation Consortium (DVCC).[7] When opening a bank account at a financial institution, identity verification procedures are performed. Given that these procedures impose a significant burden on applicants and financial institutions, the DVCC is considering a system in which the identity verification required by the Act on Prevention of Transfer of Criminal Proceeds is issued as a VC, which can be presented by applicants to other financial institutions when needed (secondary use of identity verification results). Specifically, the applicant manages the result of identity verification made at the time of transaction with a financial institution as a VC called the "Transaction-time Identity Verification VC", and presents this VC, together with the result of identity verification conducted using the Japanese Public Key Infrastructure (JPKI), etc (the "Signature Verification Result VC"), to another financial institution with which the applicant is trying to open a new bank account. Through the use of these two VCs, the DVCC aims to achieve both rigor and convenience in account opening practices.

The second example is the application of VCs to commercial transactions using AI agents. An AI agent refers to a program that autonomously performs various processes and transactions based on the user's intentions or instructions. In commercial transactions, it automatically executes tasks, such as checking inventory for merchandise and processing transactions, in accordance with the user's instructions. In September 2025, Google, a major IT company, announced the "Agent Payments Protocol (AP2)", a framework for enabling secure commercial transactions by AI agents.[8] By utilizing AI agents in commercial transactions, the framework aims to enable users to, for example, search for the most suitable products across multiple online stores and purchase them securely and conveniently. AP2 uses three types of VCs, called "Mandates," at each stage of a commercial transaction - confirming the user's intent, checking the product's price and availability, and executing the payment - to reliably confirm the details of information processing, thereby preventing AI agents from executing actions that contradict users' instructions and ensuring that a reliable record of the transaction process is maintained, ultimately ensuring the security of the overall transaction (Figure 4).[9]

[Figure 4] An overview of Google AP2



(Note) Prepared by the authors based on Google's website and other sources.

In the emerging domain of commercial transactions using AI agents, VCs are considered capable of being a fundamental technology that ensures security and reliability.

Initiatives for further utilization of VCs are being promoted not only by the private sector but also by governments around the world. In Japan, the Digital Agency established an advisory panel for further utilizing VCs[10] in 2025. Currently, a separate advisory council[11] is examining issuing copies of residence certificates and employment certificates as use cases and analyzing issues that would arise if these certificates are issued as VCs. In Europe, the introduction of the "EU Digital Identity Wallet (EUDIW)" is scheduled by the end of 2026, with the aim of storing users' digital certificates on devices such as smartphones to enhance the convenience of administrative procedures and private-sector services. VCs have been adopted as the technology underpinning certificates stored in the EUDIW. Multiple pilot experiments have been carried out for the introduction of the EUDIW. In a pilot experiment called "POTENTIAL,"[12] demonstration trials were conducted in 19 EU member states and Ukraine across six domains, such as opening bank accounts and issuing driver's licenses, involving more than 140 participating organizations from the public and private sectors. Efforts are underway for the introduction of the EUDIW by the end of 2026, including developing an implementation framework and legal and regulatory arrangements.

Trends in Standards Development and a Concrete Example of VCs

Looking at trends in standardizing VCs, the World Wide Web Consortium (W3C) introduced the concept of verifiable information in 2017.[13] It then published the "Verifiable Credentials Data Model 1.0" as a recommendation in 2019 for standardizing fundamental mechanisms for VCs. In 2025, the Internet Engineering Task Force (IETF) released "Selective Disclosure for JSON Web Tokens" (RFC 9901), which adds selective disclosure capabilities to the JSON Web Token (JWT), a standard for signing and encrypting data. Furthermore, the OpenID Foundation published standards in 2025, including "OpenID for Verifiable Credential Issuance 1.0 (OID4VCI)," which defines a VC issuance protocol, and "OpenID for Verifiable Presentations 1.0 (OID4VP)," which specifies a VC presentation protocol. In addition, the ISO/IEC Joint Technical Committee 1 (JTC 1) published an international standard for mobile driver's licenses that also supports offline use as ISO/IEC 18013-5 in 2021, and has been developing the ISO/IEC 23220 series as more generalized standards.

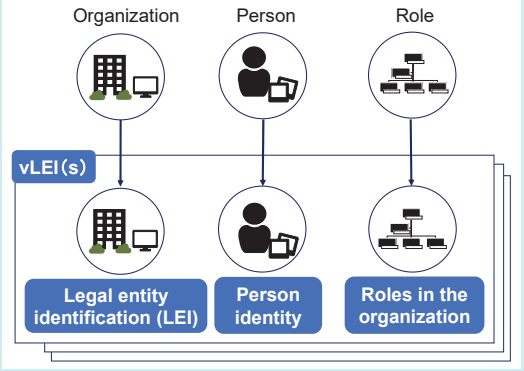
As an example of standards development for VCs, the following section introduces the verifiable Legal Entity Identifier (vLEI),[14] published as an international standard (ISO 17442-3) in October 2024 by ISO/TC 68 (the ISO Technical Committee on Financial Services), for which the Bank of Japan serves as the secretariat of the national committee.[15] A key feature of vLEIs is that, as described below, a trust-chain structure headed by the Global LEI Foundation (GLEIF), a non-profit organization, has been established, thereby clearly defining the governance structure of the entire ecosystem.

Overview of the vLEI

The vLEI is based on the Legal Entity Identifier (LEI).[16] The LEI is an international identifier used to identify counterparties to transactions of financial instruments, such as legal entities and funds. It is expressed as a 20-character alphanumeric code. Currently, the LEI is used not only for the reporting of over-the-counter derivatives transactions—the original purpose for which it was established—but also across a wide range of domains, including other financial fields such as settlement instructions and non-financial fields such as trade.

The vLEI is a framework that links various VCs that represent a legal entity's identity, including its LEI code, the identity of its officers, and the roles they perform in the organization. Intuitively, a vLEI can be understood as a "digitally and cryptographically signed and sealed envelope", associated with a transaction, that contains the legal entity information (LEI) as well as the names and titles of the entity's officers (Figure 5).

[Figure 5] Conceptual diagram of the vLEI

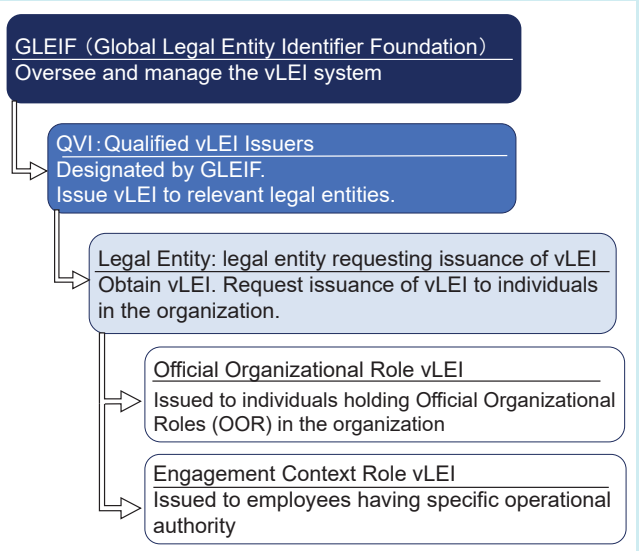


(Note) Prepared by the authors based on the GLEIF website and other sources.

One of the features of the vLEI is that GLEIF is responsible for governing the entire vLEI ecosystem, providing the foundation for the trust chain — a mechanism through which trust relationships can be verified by tracing connections, such as digital signatures. For general VCs, while the authenticity of the certificate can be guaranteed, ensuring the trustworthiness of the VC issuer is a challenge. For the vLEI, however, GLEIF manages the vLEI ecosystem in a digitally verifiable manner, which enhances the reliability of the vLEI by assuming governance of the entire system.

The vLEI trust chain operates as follows: GLEIF designates Qualified vLEI Issuers (QVIs) and issues vLEIs for QVIs; QVIs then issue vLEIs to the relevant legal entities; and either QVIs or the legal entities issue vLEIs related to officers' roles (Official Organizational Role vLEI and Engagement Context Role vLEI) to the officers.[17]

[Figure 6] The vLEI trust chain



(Note) Prepared by the authors based on materials from the Bank of Japan's 9th ISO Panel and other sources.

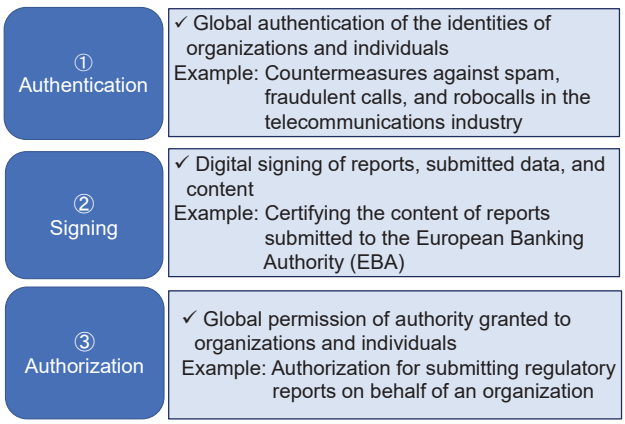
In this way, issuing vLEIs at each layer creates a trust chain under a nested structure. This is a key feature of the vLEI. When verifying a downstream vLEI (e.g., Official Organizational Role vLEI), it is possible to verify the authenticity of credentials by also including information from upstream layers (such as the relevant entity's vLEI) .

Another feature of the vLEI is that the vLEI uses different technologies from those employed in VCs designed for individual use. The vLEI employs distinctive technologies, in terms of data format, security,[18] and data transmission and representation,[19] to establish and verify the trust chain described above. For example, regarding the data format, the vLEI adopts the technology called Authentic Chained Data Containers (ACDC). This enables the establishment of a nested structure with various vLEIs and the storage of multiple signed credentials. Moreover, since these technologies do not necessarily require external ledgers, such as blockchains, they enable self-contained verification of the trust chain, thereby enhancing the stability of the entire ecosystem.

Trends in the Utilization of vLEIs

There are three main functions of the vLEI: (i) authentication of identities of organizations and individuals; (ii) signing of organizations' and individuals' reporting data and content; and (iii) authorization granted to organizations and individuals (Figure 7).

[Figure 7] Functions of the vLEI



(Note) Prepared by the authors based on materials from the Bank of Japan's 9th ISO Panel and other sources.

By providing these functions in a machine-readable form, vLEIs are expected to prevent risks such as impersonation and credential falsification, and to enable the automation of transaction processing.

At present, eight companies have been designated globally as QVIs by GLEIF,[20] and efforts for specific applications of the vLEI that leverage the above three functions are progressing. Concrete initiatives are being pursued not only for utilization in typical financial domains,[21] such as reporting to regulatory authorities, but also for a wide range of purposes, including caller authentication in telecommunications to counter nuisance and fraudulent calls, supply chain management (authenticity is guaranteed through signing on transactional documents and data), and trade finance transactions (verifying the identities and authority of transaction participants using vLEIs to reduce customer screening costs).

Conclusion

This report has provided an overview of VCs, which have attracted increasing attention amid the advancement of digitalization, and has outlined their key technological features and use cases. Furthermore, the report has surveyed the development of VC-related standards by various industry associations and standardization organizations, and has introduced the vLEI as an example, for which an international standard was published in October 2024.

VCs are an emerging technology that is expected to offer significant potential. At the same time, consideration from a wide range of perspectives is required for envisioning the further utilization of VCs. For instance, on the technological side, while various industry associations and standardization organizations have been proceeding with the standardization of VCs, resulting in a range of standards and data formats suited to different purposes, the coexistence of these multiple standards and formats raises the issue of ensuring interoperability. On the operational side, as mentioned above, in addition to challenges related to ensuring the trustworthiness of the issuance made by legitimate issuers, proper operational processes are required throughout the entire lifecycle, even after issuing a VC, including managing validity periods, updates, reissuance due to attribute changes, and even revocation management. Beyond these aspects, to further utilize VCs, it is necessary to carefully consider the risks associated with their adoption and relevant countermeasures.

In a digital society, the ability to prove one's identity in a secure, reliable, and convenient manner is considered a critical factor for the future of finance and payments. In particular, with the continued advancement of digitalization, various types of money are anticipated to move across borders at unprecedented speeds. Under such circumstances, the need to securely, reliably, and conveniently prove or verify the information of individuals and companies involved in sending and receiving money is likely to increase as well. VCs could contribute to this need.

Going forward, the Bank of Japan, as the secretariat of the ISO/TC 68 national committee, will continue to closely monitor technological developments related to VCs, as well as discussions on their practical use.

---

[1] While the "Verifiable Credentials Data Model v2.0" by the World Wide Web Consortium (W3C) defines a VC as "a tamper-evident credential whose authorship can be cryptographically verified," this report defines a VC in a way that is easy to understand even for readers who are unfamiliar with VCs.

[2] The "Verifiable Credentials Implementation Guidelines 1.0" by W3C defines software where users store VCs as a "Repository" and it presents a wallet as one example of such software.

[3] In a VDR, in addition to public keys, information necessary for verifying VCs is registered, including definitions of the data structure (known as schemas) and revocation information of VCs. The W3C's Verifiable Credentials Data Model v2.0 states that information registered in a VDR is expected to enable the detection of tampering and serve as an accurate record of who manages what data.

[4] As discussed later, for general VCs, it may not be fully guaranteed that a VC has been issued by a legitimate issuer; in other words, the possibility that the VC was issued by an illegitimate issuer cannot be ruled out. In such cases, additional measures are required to ensure the trustworthiness of issuers, like the preparation of a list of trusted issuers (trust list).

[5] Mobile driver's licenses in the U.S. are issued based on the international standard ISO/IEC 18013-5. The Mobile Driver's License Implementation Guidelines have been published by the American Association of Motor Vehicle Administrators (AAMVA).

[6] In contrast to this feature, explanatory materials of the secretariat of the Digital Agency's "Advisory Council on Issues of Attribute Certification (1st meeting)" (https://www.digital.go.jp/councils/vc-diw-governance/2c9c78e4-4cb5-4ef0-a3e5-6fd461d0ef84) also point out that "Since a VC contains information that is easily used for cross-referencing (such as the Issuer's signature value), if multiple Verifiers intentionally share VCs and conduct cross-referencing, there is a risk that privacy may be violated."

[7] For DVCC initiatives, refer to the minutes and materials of the Digital Agency's "Advisory Panel on Governance in the Use of Verifiable Credentials (VC/VDC) (1st meeting)" (https://www.digital.go.jp/councils/verifiable-credential-governance/5a5c145f-85f4-41a5-bc51-4e442c6154b8).

[8] For an overview of AP2, refer to Google's website (https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol?hl=en).

[9] AP2 supports two models: Human Present and Human Not Present. Figure 4 illustrates an overview of the former.

[10] Refer to the materials stated in footnote 7.

[11] The Digital Agency's "Advisory Council on Issues of Attribute Certification" (https://www.digital.go.jp/councils/vc-diw-governance).

[12] For initiatives in POTENTIAL, refer to the website at https://www.digital-identity-wallet.eu/.

[13] The W3C established a working group in 2017 to standardize a data model and representations for "Verifiable Claims (later Verifiable Credentials)." Then consideration for its concrete implementation was carried out.

[14] Commissioned by the Japanese Industrial Standards Committee (JISC), a council set up under the Ministry of Economy, Trade and Industry, the Bank of Japan's Payment and Settlement Systems Department acts as the secretariat of the national committee of the ISO/TC 68. For initiatives of the ISO/TC 68 national committee and other information, refer to the webpage at https://www.boj.or.jp/paym/iso/index.htm.

[15] The Bank of Japan's Payment and Settlement Systems Department held the ISO Panel (9th): Potential Use of the Legal Entity Identifier (LEI) Expanding from Market Reforms for Over-the-Counter Derivatives to Foreign Exchange Operations and other areas." (https://www.boj.or.jp/paym/iso/iso_panel/isop250228.htm) in February 2025. In

addition to explanations by GLEIF of vLEI, a panel discussion was conducted covering general aspects of LEI, including vLEI.

[16] The LEI was established based on the lessons learned from the financial crisis following the collapse of Lehman Brothers, which showed that the inability to gain a macro-level understanding of the actual status of global over-the-counter derivatives transactions delayed the close-out of the trades and exacerbated the crisis. The operation of LEI codes is managed by GLEIF, which is overseen by the Regulatory Oversight Committee, composed of financial authorities and central banks. The LEI was standardized as ISO 17442 in June 2012. For an overview of the LEI and the background of its introduction, refer to "Current Status of International Discussions on Corporate ID Numbers Used in Financial Services" (Bank of Japan Review 2019-J-7, 2019) by Hashimoto, T. (https://www.boj.or.jp/research/wps_rev/rev_2019/data/rev19j07.pdf).

[17] The Official Organizational Role vLEI is a vLEI issued based on the official role of an individual representing an organization or legal entity, as specified by the international standard ISO 5009. However, the Engagement Context Role vLEI is issued for other roles in the organization (e.g., chief risk officer). Both vLEIs contain information about the relevant legal entity. However, it should be noted that the Official Organizational Role vLEI is issued by QVIs, whereas the Engagement Context Role vLEI can be issued by either QVIs or the relevant legal entity.

[18] To ensure security, the technology called Key Event Receipt Infrastructure (KERI) is employed. KERI is designed so as not to require reliance on external blockchains or other systems, ensuring flexibility in the scope of its application. In addition, it incorporates a process called "pre-rotation," where the next key to be used is determined and "reserved" in advance, to make it difficult for a private key to be used for impersonation even if the key is stolen.

[19] For data transmissions and representations, the technology called Composable Event Streaming Representation (CESR) is employed. The format of the data, including cryptographic information like signatures (used for tamper detection and identity verification), is strictly defined, ensuring that the data structure and information necessary for verification remain intact, and it supports operations that are suitable for methods where continuous data are read and processed sequentially, as well as machine processing.

[20] For the list of QVIs, refer to GLEIF's website (https://www.gleif.org/ja/organizational-identity/get-a-vlei-list-of-qualified-vlei-issuing-organizations). In Japan, TOPPAN Edge Inc. was designated as a QVI in September 2025.

[21] The European Banking Authority (EBA) carried out a pilot experiment using vLEIs from 2024 to 2025 to respond to new reporting requirements concerning disclosures under Basel regulations (the so-called Pillar 3). This experiment explored the use of vLEIs to manage reporters' identities in an efficient and tamper-proof manner while reducing the operational burden for both financial authorities and financial institutions.

The Bank of Japan Review Series is published by the Bank to explain recent economic and financial topics for a wide range of readers. This report, 2026-E-6, is a translation of the Japanese original, 2026-J-2, published in March 2026. Views expressed are those of the author(s) and do not necessarily reflect those of the Bank. If you have any comments or questions, please contact the Information Technology Standardization Group, Payment and Settlement Systems Division, Payment and Settlement Systems Department (E-mail: post.pr@boj.or.jp). The Bank of Japan Review Series and the Bank of Japan Working Paper Series are available at https://www.boj.or.jp/en/index.htm.