

GLEIF Response to Payments NZ's Consultation on Payments for the Next Generation

March 28th, 2025

The Global Legal Entity Identifier Foundation (GLEIF) appreciates the opportunity to respond to Payments NZ's consultation on modernizing the payments ecosystem in New Zealand. We acknowledge and support the Payments NZ initiative to explore the next generation digital payments capability for Aotearoa in the future. As GLEIF is specialized in global identity management, our responses are mainly focused on issues related to identity and its implications for the architecture to support innovative solutions, the role of the payment system in the digital economy and to address regulatory and compliance requirements.

First, a brief introduction of GLEIF:

Established by the Financial Stability Board in June 2014, the [Global Legal Entity Identifier Foundation \(GLEIF\)](#) is tasked to support the implementation and use of the [Legal Entity Identifier \(LEI\)](#). GLEIF is a supra-national not-for-profit organisation headquartered in Basel, Switzerland. The Global LEI System is overseen by over 70 public authorities participating in the [Regulatory Oversight Committee](#). GLEIF's mission is to promote transparency, trust, and efficiency within global financial markets by enabling the implementation and use of the Legal Entity Identifier (LEI) and vLEI (verifiable LEI) solutions. We bring extensive experience working with financial market infrastructure providers, regulators, and market participants to establish standardized, interoperable identity frameworks that enable secure and efficient data exchange.

The LEI is based on ISO17442 standard. It is a global and machine-readable standard for the unique legal identification of legal entities worldwide. It consists of a 20-digit, alpha-numeric code that enables clear and unique identification of legal entities. The code is linked to a set of key reference information relating to the legal entity in question e.g., name, legal form,

headquarter address, parent company, child entities. This enables clear and unique identification of legal entities participating in trade and financial transactions, including their ownership structure. Below is an example LEI of an entity registered in New Zealand:

<https://search.gleif.org/#/record/9845004A5AA41I6BNC94>. GLEIF operates under the Open Data Charter terms, which means that the complete database of LEIs and the associated LEI reference data is available free of charge for anyone to access. GLEIF makes the LEI and LEI reference data available via full file download, webpage search and API.

Building upon the success of the LEI, GLEIF has introduced the [verifiable Legal Entity Identifier \(vLEI\)](#). The vLEI is a digitally verifiable credential (VC) that contains the LEI and enables organizations to create secure, digitally authenticated credentials for their official representatives and contextual business roles. By using advanced cryptographic techniques, the vLEI provides a verifiable identity that is secure, interoperable, and can be authenticated in real-time across a multitude of platforms and jurisdictions. The vLEI provides a mechanism to manage identity as infrastructures transition towards ledger-based instruments including CBDC, smart contracts and tokenised assets.

GLEIF would like to address below questions in our below response:

Consultation question 2

In your view, what future strategic capabilities should be prioritised in the design of a next gen ecosystem? What else should we be considering?

Consultation question 9

Where do you see your role or your organisations role in the forming of a next gen payment capability?

Consultation question 11

What pieces of the ecosystem, or developments currently in-flight are critical to progressing payments modernisation activity (e.g. digital identity, tokenisation, regulation)?

Consultation question 18

To what extent do you agree/disagree with our assessment of a scheme framework?

What changes, if any, should be made to further develop the approach?

Consultation question 20

To what extent do you agree/disagree with our assessment of a payments data strategy?

What changes, if any, should be made to further develop the approach?

Consultation question 26

To what extent do you agree/disagree with the problem definition attached to digital identity? What changes, if any, should be made to further develop the problem definitions?

Consultation question 27

To what extent do you agree/disagree with the benefits of the verifiable credentials service?

What changes, if any, should be made to further develop the benefit statements? And what impacts do you foresee for the people and businesses of Aotearoa as a result?

Addressing Question 2, GLEIF appreciates the comprehensive and far-sighted scope of issues that NZ Payments seeks to address. GLEIF collaborates closely not only with standard setters and central banks but also actors driving the adoption of new infrastructures and services in digital assets and the broader digital economy. In this context we concur on major trends and forces reshaping the payment landscape. Given the mandate of GLEIF to provide universal solutions to organisational identity, including in the evolving digital economy, we would highlight in particular the need for Payments NZ to plan for capabilities that address:

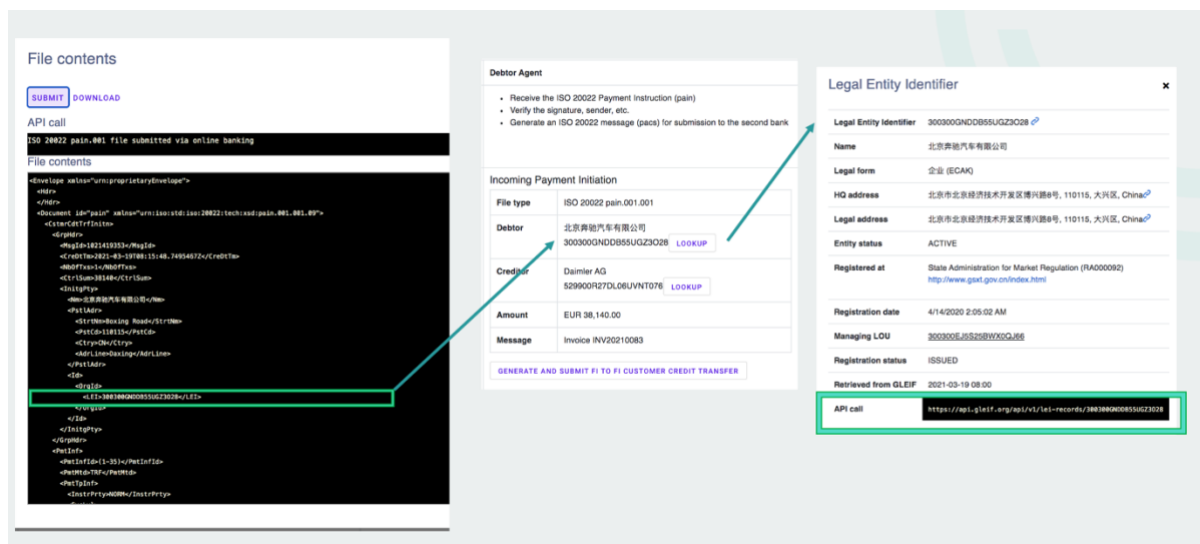
- **Growth and evolution of the digital economy:** as a small, open economy, New Zealand is likely to see disproportionate growth in the export and import of digital products and services and businesses, also SMES, that operate across national borders. So alongside the need to address P2P and consumer payment services, there is likely to be growth in the volume and demand for a variety of cross-border B2B payments services and ancillary functions. Business processes in the digital economy are now often generating subtasks that span borders, generating more complex, interdependent payment chains for the delivery of digital goods and services.

- **Emergence of new International and cross-border infrastructures:** New regional and international payments systems will enhance the need for interoperability and integration between different payment ecosystems. This entails being able to operate using multiple and ideally also internationally accepted standards for messaging, scheme rules, counterparty authentication and authorisations, identification and non-payment processes such as for compliance.
- **Incremental, orderly integration of ledger-based infrastructures:** Formal, regulated financial market infrastructures are gradually adapting to and embracing permissioned and distributed ledger architectures that enhance interoperability across historical silos and support decentralisation. This trend will continue and will require compatible changes in retail and business-oriented payment systems, nationally and for cross-border transactions. We believe payment systems need to plan for a world in the future that require identifiers and data credential tools that are compatible with on and off-chain operations and interoperable across different networks, as articulated in the Finternet Whitepaper of the BIS.

Addressing **Question 9**, GLEIF believes that our role in shaping next-generation payment capabilities is centered on **enhancing the identity layer of the payments ecosystem**, through the LEI as a global entity identification layer and the vLEI as a trusted and verifiable digital identity framework.

Addressing **Question 20**, GLEIF fully supports Payments NZ's approach of developing a coherent and future-proofed payments data strategy, particularly the adoption of ISO 20022 and open data standards. The integration of structured, information-rich payments data will be a foundational enabler of next-generation payments capabilities, fostering efficiency, transparency, and security across the ecosystem. GLEIF would like to propose **the adoption of the LEI as a data element within the payment data strategy for identifying legal entities involved in financial transactions (e.g. originator, beneficiary)**. This will enable:

- Smooth alignment with ISO20022. ISO 20022 already incorporates LEIs as a standard entity identifier, making it an ideal tool for enhanced payment data structuring and regulatory reporting. Below is an example (Figure 1):



- Global interoperability. The LEI is being globally recognized and adopted by many jurisdictions in the context of domestic and cross-border payment. For example,
 - the Financial Stability Board¹ put its full weight behind a landmark recommendation in 2022 that the LEI should be widely adopted across the global payments' ecosystem. Global standards-setting bodies and international organizations with authority in the financial, banking, and payments space were encouraged to drive forward LEI references in their work.
 - The FATF recently released the second consultation² on revision of Recommendation 16, in which it specifies the usage of identifiers (including the LEI) to identify originator and beneficiary legal persons.
 - Bank of England mandates the adoption of LEI starting from financial institutions in their CHAPS system when migrating to ISO20022³.

¹ FSB, 2022, Options to Improve Adoption of The LEI in Particular for Use in Cross-border Payments, available at: <https://www.fsb.org/wp-content/uploads/P070722.pdf>

² FATF, 2025: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-February-2025.html>

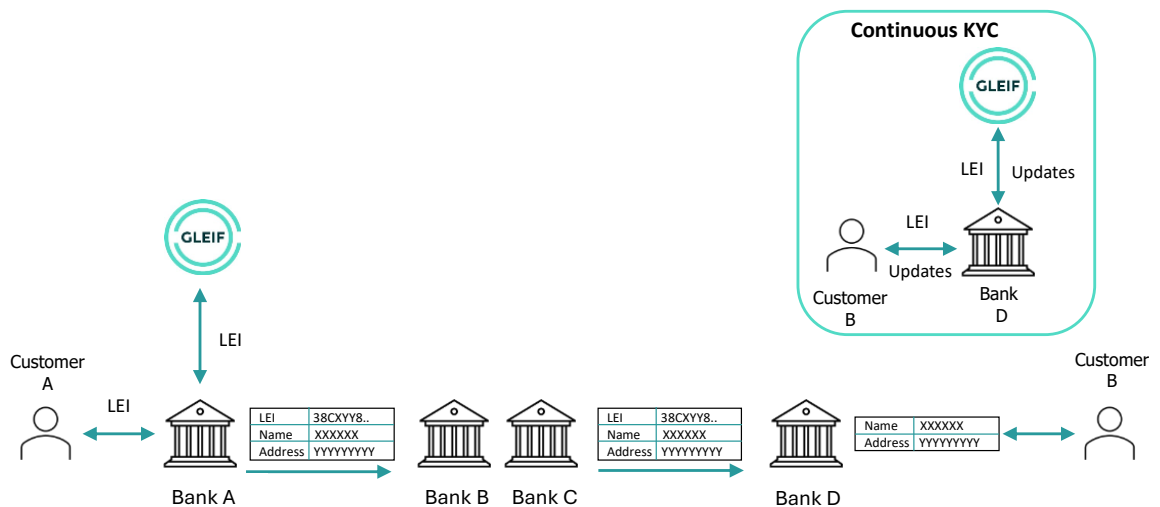
³ Bank of England, 2024, Policy Statement: Mandating ISO 20022 Enhanced Data in CHAPS, available at: <https://www.bankofengland.co.uk/paper/2024/policy-statement/mandating-iso-20022-enhanced-data-in-chaps>

- Reserve Bank of India (RBI) issued a mandate for the LEI in all payment transactions totaling ₹ 50 crore and more undertaken by entities for Real-Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT).
- Precise identification of payer and payee entities. Data structuring requirements, as suggested by the CPMI, require the unique identification of all entities involved in cross-border payments in an internationally recognized and standardized manner. These requirements suggest the use of the LEI as an identifier, benefiting cross-border payments by facilitating validation and screening processes. This in turn will reduce the number of "false positives" flagged by compliance screening filters utilized for sanctions checks and AML screening. Eliminating ambiguity in the identification of entities makes payments more transparent, which results in reducing the cost of cross-border payments via fewer manual interventions to identify financial institutions are required.

Below is an example payment flow taken from the CPMI "ISO 20022 harmonization requirements for enhancing cross-border payment"⁴. This payment flow is adapted to demonstrate the integration of the LEI and technical tools like the GLEIF API. The table under the graphic describes the recommended actions of involved parties. This example payment flow describes the ideal market practices for Financial Institutions (FIs) implementing the LEI for creditor/debtor identification.

Figure 2: LEI to be used in ISO 20022 Confirmation of Payee (CoP)

⁴ <https://www.bis.org/cpmi/publ/d218.pdf>



Responsibilities of the involved parties

Customer A	<ul style="list-style-type: none"> - Ensure all suppliers are onboarded and tagged with the LEI. - Provide the LEI of the supplier (beneficiary) in the payment order.
PSP A/Bank A Debtor Agent	<ul style="list-style-type: none"> - Technically enable transmission of the beneficiary LEI in the PSP interfaces. - Request Customer A to confirm the name and address associated with the LEI are the intended name and address for the recipient. - Upon confirmation by Customer A, pass the LEI name and address in the payment message.
Bank B	- Pass payment information.
Bank C	- Pass payment information.
PSP B/ Bank D Creditor Agent	- Confirm that the LEI, name and address in the payment message matches the information associated with the beneficiary account.
Customer B	- Obtain LEI and maintain its policy conforming status

While adopting the LEI, it can be presented via a QR Code. Consumer/Business can verify the beneficiary with the LEI without any language limitations as the QR code entails all the information, including the legal name and legal address of the company. Below is an example QR code linking to entity Hitachi, Ltd.'s LEI information (Figure 3):



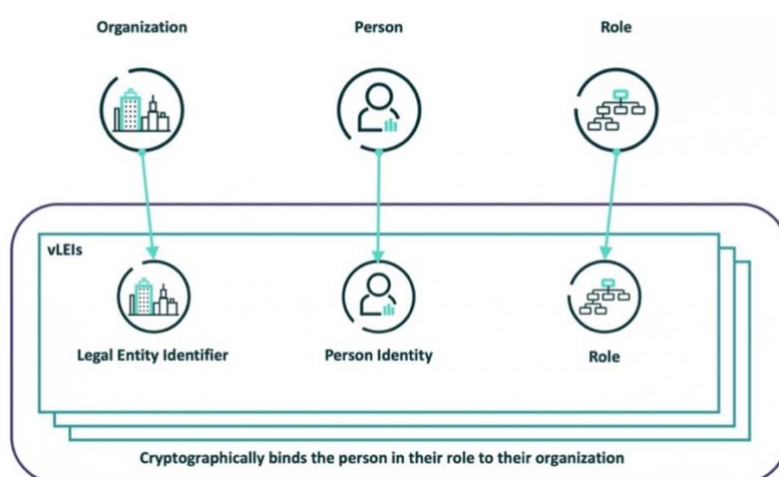
Addressing **Question 11 and 18**, GLEIF believes that digital identity is critical to progressing payments modernisation activity and shall play a fundamental role. Identity serves as the foundation for all transactions and interactions within the payments ecosystem, particularly in an increasingly digital world where trust must be established before any activity can take place. From an even broader perspective, digital identity shall be the cornerstone for all trusted digital interactions and data exchanges, not only limited to payments. Therefore, we propose that digital identity shall not only be considered under scheme framework, but also be considered on a technical level in the centralised operational platform.

Addressing **Questions 26 and 27**, GLEIF agrees with the proposal to integrate the capabilities represented by Verifiable Credentials (VCs) into the next-gen payments ecosystem. Growing sophistication and inter-connectedness of financial and commercial operations will drive the adoption of programmable payments and smart contract type operations. These developments will require many more checks and data verifications, e.g. not only of payee or payer identity but also a growing array of features, for example, events that may trigger contractual payments, confirmation of ownership or signing rights, or for instance escrow service. We expect both legal and natural persons to gradually adopt and increasingly issue and use different kinds of verifiable credentials, data wallets and data exchange protocols to present, verify, as well as chain or link data, attestations or other credentials to support commercial transactions that operate across networks, including payment systems. The demand of this envisioned future state is one of the reasons also why GLEIF has developed the verifiable LEI (vLEI). The vLEI serves not only as an interoperable,

verifiable form of digital identity credential; it also supports the chaining (or inter-linking) of credentials and attestations issued to legal persons and their representatives from different sources. Therefore, GLEIF **recommends Payments NZ to consider the role of the verifiable LEI (vLEI) as an interoperable digital organizational ID standard that also supports the broader digital and data ecosystem..**

The [verifiable LEI \(vLEI\)](#) is developed by adding the LEI into verifiable credentials. This is being released as ISO 17442-3 standard in October 2024. The vLEI (verifiable LEI) represents the next step in self-sovereign identity for legal entities. As a digitally verifiable credential, vLEI authenticates an individual and his/her affiliation with or rights assigned to them by a legal entity. For example, the CEO of a legal entity obtains a vLEI credential to prove he/she is the legal representative of the entity and is able to conduct authorized signing of the entity's payment instructions or orchestrate the signing of multiple signatories from within the company; an employee of a legal entity can be issued by the company with a specific "engagement role" vLEI credential to prove that he/she is authorized, for instance, to request a payment or sign an agreement on behalf of the entity.

Figure 4: vLEI credential linking individual and organization with role



The vLEI enables data privacy and controlled data sharing objectives to be achieved in line with the expectations raised in the section of the consultation on Data Governance. The vLEI architecture follows the popular "never trust, always verify" mantra, embodied by the counterintuitively labelled "Zero Trust Architecture" movement, which is rapidly growing within the cybersecurity industry. The vLEI infrastructure is a network-of-networks of true universality and portability, developed using the KERI (Key Event Receipt Infrastructure)⁵ protocol. It supports the full range of blockchain, self-sovereign identity and other decentralized key management platforms. vLEIs will be hostable on both ledgers and cloud infrastructure supporting both the decentralization of ledgers plus the control and performance of cloud. Portability will enable GLEIF's vLEI ecosystem to unify all ledger-based ecosystems that support the vLEI.

GLEIF has based the design of the vLEI on the Authentic Chained Data Container (ACDC) developed within the Trust over IP Foundation (which is hosted by the Linux Foundation). The ACDC enables users to manage an array of data, tokenized credentials and attestations to be verified, shared and linked or chained. This choice of architecture reflects recognition of the differences for instance between the function of government identity wallets for natural persons and the more specific and sophisticated needs and challenges related to organizational identity, the roles of employees within them and the management of legal entities signing rights and data operations. GLEIF would be pleased to share more information about the specific design issues and architecture choices related to verifiable credentials.

The vLEI as an overarching trust framework will not be directly in scope of accreditation under the Digital Identity Services Trust Framework (DISTF)⁶, however, GLEIF believes that as this framework meet the identification standards set up by DISTF, it will facilitate

⁵ <https://keri.one/>

⁶ <https://www.digital.govt.nz/standards-and-guidance/identity/trust-framework>

accreditation of the vLEI services and solutions provided by potential Qualified vLEI Issuers (QVIs)⁷, who are qualified by GLEIF to issue and maintain vLEI credentials.

For example,

- Information Assurance standard requests ‘Robustness of the process to establish the quality and accuracy of Entity Information’ ->>

The LEI data, containing reference information of an entity, is being managed by a robust [data quality management](#); and the [vLEI governance framework](#) offers a controlled and audited methodology of the whole lifecycle of the digital identity credential;

- Authentication Assurance standard requests ‘Robustness of the process to ensure an Authenticator remains solely in control of its holder’ ->>

The [vLEI governance framework](#) details reliability requirements in the primary document: [verifiable LEI \(vLEI\) Ecosystem Governance Framework Primary Document; Meanwhile, the](#) Authentic Chained Data Container (ACDC) credential is cryptographically secure, [which ensures the](#) authentication method is used and controlled only by the authorized person, preventing unauthorized access or tampering.

The vLEI credentials enable below four core functions:

- **Digital signing:** Authorized signatories or other authorized individuals could use the vLEI credential to digitally seal or sign data.
- **Authentication:** Verification of the cryptographic validity of the vLEI credential and signature.
- **Permissioning:** Confirmation that a legal entity, or representative of this legal entity is authorized to access a system or to perform an action.
- **Credential Chaining:** enabling legal persons and their representatives to link and combine verifiable credentials or attestations from different sources without breaking the chain of trust needed to trace provenance and verify integrity of underlying data.

⁷ <https://www.gleif.org/en/vlei/get-a-vlei-list-of-qualified-vlei-issuing-organizations>

With the above functions, the vLEI in combination with the LEI forms a strong foundation of digital identity for payment ecosystems and the evolution of smart contract based commercial and financial ecosystems. Using the above figure 2 as an example,

- Bank A onboards Customer A as their corporate client
- Bank A identifies Customer A via their LEI;
- Bank A issues vLEI credentials to Customer A's Legal Representative;
- Bank A issues vLEI credentials to Customer A's Staff;
- Customer A's Legal Representative and Staff use their vLEI credentials to log into Bank A's online platform;
- Customer A's Legal Representative use its vLEI credential to sign a large-volume payment instruction to Customer B at Bank D;
- Customer A's Staff use its vLEI credential to request a small-volume payment.
- When receiving the payment instruction, Bank D verifies the LEI of Customer B on payment instruction is consistent with the LEI on Bank D's profile.

In this example, the vLEI credential ensures cryptographic verification of identities, significantly reducing fraud risks, unauthorized access, and payment misdirection. Using the vLEI for digital signing guarantees the authenticity and integrity of payment instructions, preventing unauthorized modifications. Banks and financial institutions can instantly verify corporate clients, their legal representatives, and their staff, ensuring payments are initiated only by authorized individuals.

Above are some proposals GLEIF would like to provide to Payments NZ in the context of digital identity adoption for the next gen payment system. GLEIF believes that incorporating LEI and vLEI into the next generation payments ecosystem for New Zealand can greatly enhance trust, security, and interoperability. By leveraging these globally recognized standards, Payments NZ can address many of the key objectives outlined in the consultation paper, including promoting innovation, meeting regulatory expectations, and improving accessibility. GLEIF welcomes further engagement with Payments NZ to explore these recommendations in greater detail.