



Trusted Identities for a Trusted Web: LEI and vLEI in the Digital Certificate Ecosystem

This keynote will present how the Legal Entity Identifier (LEI) and verifiable LEI (vLEI) can enhance digital trust across the internet.

- ISO 17442-2 (LEI in X.509),
- ISO 17442-3 (LEI in Verifiable Credentials),
- ISO 5009 (official organizational roles).

2025-10-15

Global Legal Entity Identifier Foundation

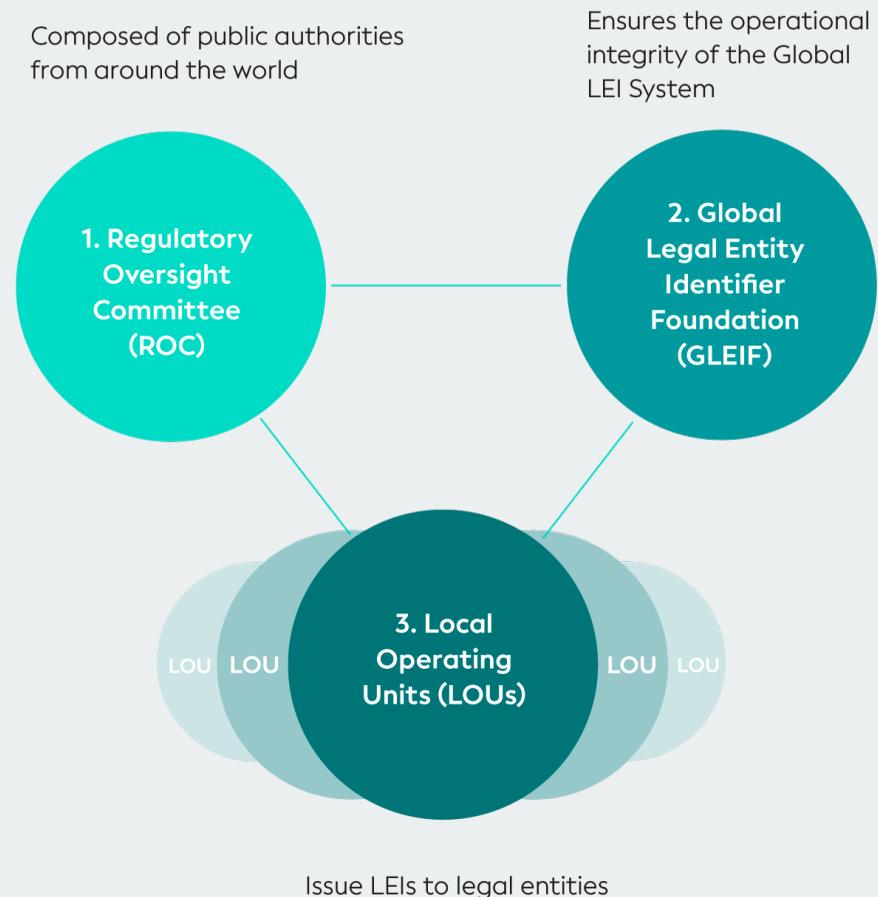
Agenda

1. GLEIF introduction
2. LEI in X509 digital certificates ISO 17442-2
3. vLEI verifiable credentials ISO 17442-3
4. Official organizational roles - ISO 5009
5. Use cases for Japan
6. Use Case for CFCA
7. Use Case for Certizen



Introducing the Global LEI System

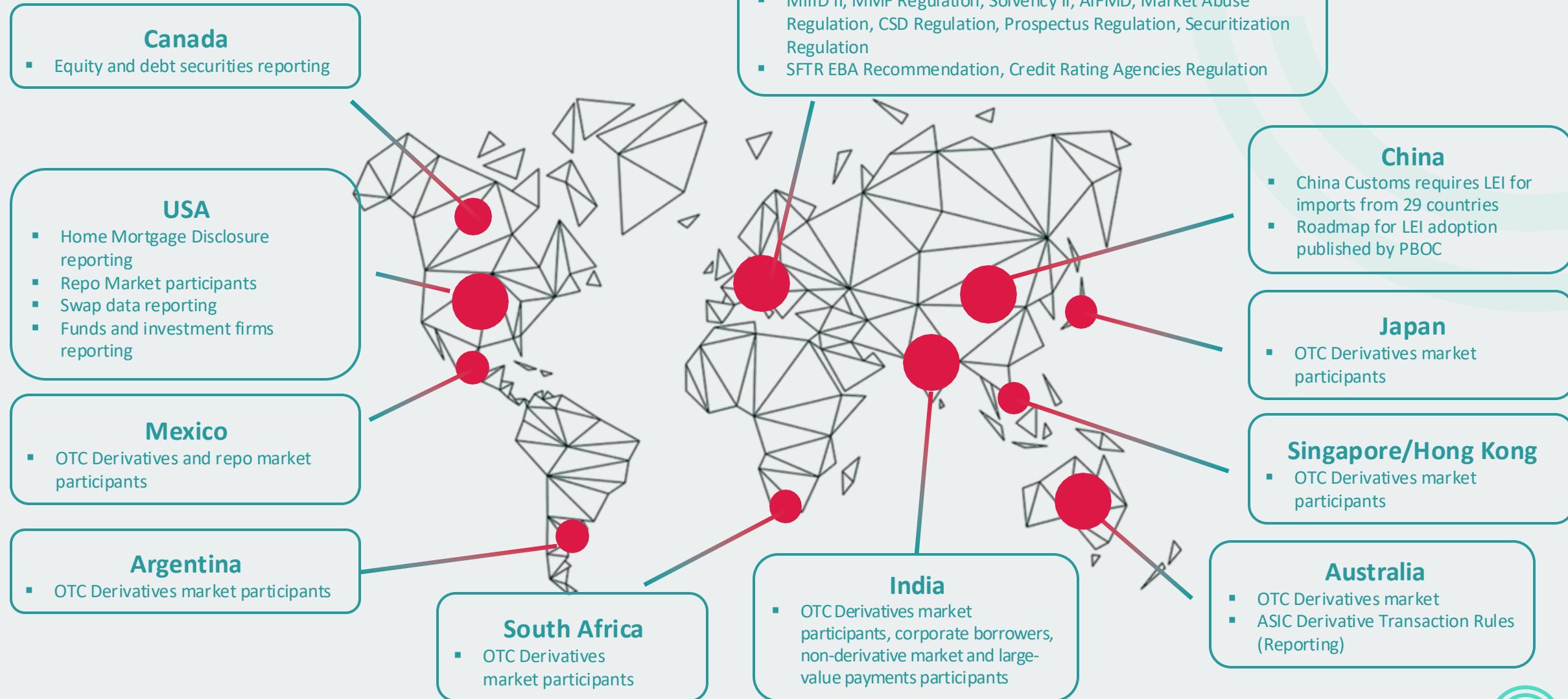
The Financial Stability Board (FSB) and the Group of Twenty (G20)
have endorsed the LEI, Global LEI System and GLEIF.



The Passport for Legal Entities



Organizational Identity in Global Regulations



Trusted Identities for a Trusted Web: LEI in Digital Certificates x.509 - ISO 17442-2: Standards situation

- In order to facilitate the use of LEIs in digital certificates, GLEIF has worked closely with standards setting organizations such as the International Organization for Standardization (**ISO**) and the European Telecommunications Standards Institute (**ETSI**) in the EU.
- Concretely, ISO is defining the [ISO 17442-2](#) and [ETSI is defining TS 119 412-1](#). These technical standards are necessary for the certificate authority industry to embed LEIs consistently into certificates.



GLEIF LEI Digital Strategy – LEI inclusion in Digital Certificates X509 [RFC 5280](#)

Standards status quo



Abstract: The [ISO 17442-2 standard](#) informs how to structure a X.509 public key certificate with embedded LEI.

FIELD used:

Within the Distinguished Name (DN) section, LEI is used in an optional dedicated field, (1.3.6.1.4.1.52266.1)) (and .2)

Example:

LEI: “254900OPPU84GM83MG36”



Abstract: ETSI [TS 119 412-1](#) to inform how the LEI may be embedded in eIDAS compliant certificates.

FIELD used:

In the certificate within the Distinguished Name (DN) section, in the Field object identifier – OID

Example with LEI code:

OID: “254900OPPU84GM83MG36”

Advantages of LEI inclusion into Digital Certificates

- Through LEI embedded digital certificates, legal entities can perform various corporate email digital **transactions** with an **extra layer of trust**.
- Includes and **extra layer of security** by embedding the global LEI code. Enhance Security and **brand protection**.
- Enables **end-to-end automation** from establishing the authenticity and integrity of an **email** account or **document** associated with the legal entity.
- Adding LEIs into digital certificates brings an additional trust proof, as the LEI is a globally secure mechanism that **provides reliable data** for company identity.
- The company's data check can be **automated** and done consistently **regardless of the country** where the company is located and the language used.



Advantages of LEI inclusion into Digital Certificates

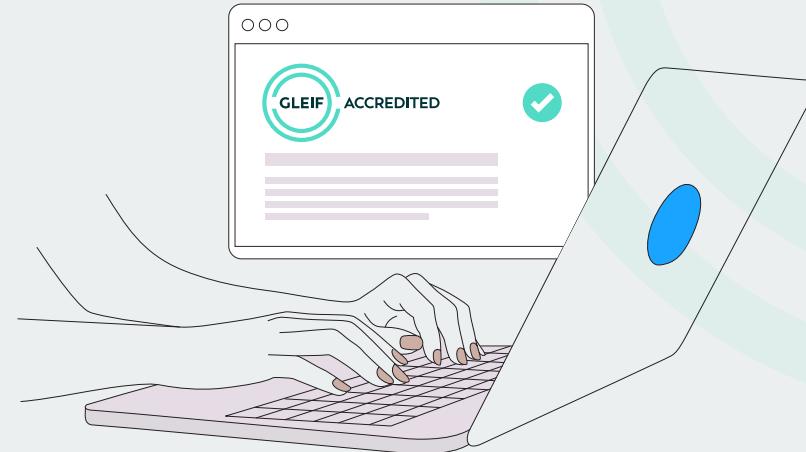
Reliability and validation of the company's data and people's identity acting on behalf of the company.

LEI connects to key reference standardised information that enables clear and unique identification of legal entities participating in financial transactions and other transactions.

GLEIF makes the historical and current LEI records available 100% for free via the **Global LEI Index**:



It is the only global online source that provides open, standardized and high-quality legal entity reference data. Any interested party can easily access and search the complete LEI data pool free of charge on the GLEIF website using the web-based LEI search tool developed by GLEIF or access records in bulk via full file download or API.

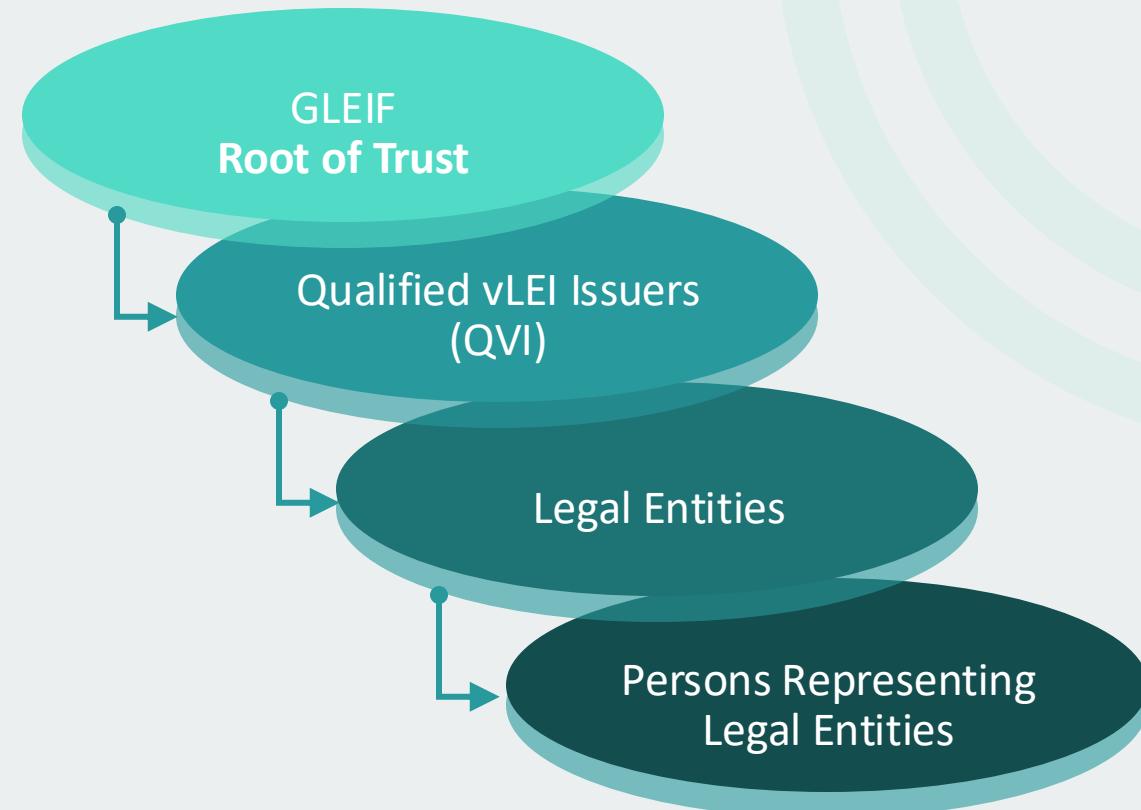


Organizational Identity: Connecting Organizations, Persons and Roles. vLEI ISO 17442-3

The LEI	The verifiable LEI (vLEI)
<ul style="list-style-type: none">■ 20-digit alphanumeric code (Example: 506700GE1G29325QX363)■ Connects to key reference data (Name(s), address(es), other identifiers)■ Provides identity	<ul style="list-style-type: none">■ Always includes an LEI■ Can in addition verifiably identify persons (or systems) in acting on behalf of the organization, or engaged with that organisation■ Enables authentication, permissioning and signing <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"><p>vLEIs</p><div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;"><p>Legal Entity Identifier (LEI Standard)</p></div><div style="text-align: center;"><p>Person Identification (String)</p></div><div style="text-align: center;"><p>Role (String)</p></div></div></div> <p>506700GE1G29325QX363</p> <p>John Doe</p> <p>CEO</p>
<p>Interoperability</p>	<p>Trust</p>

The LEI as a Verifiable Credential – the global vLEI Trust Chain

- vLEIs use self-certifying and self-sovereign **AID** (Autonomic Identifier)
- GLEIF is the **Root of Trust**
 - Root AID to establish the Root of Trust
 - Delegated AIDs to issue **Credentials**
- GLEIF established a trusted network of **Qualified vLEI Issuers (QVIs)**
- **QVIs** are qualified to issue Entity and Role Credentials ...
 - to Legal Entities
 - to Persons who represent Legal Entities either in official or functional roles
- Legal Entities can also autonomously issue (and revoke) Engagement Context Role credentials to staff, suppliers, clients, IOT devices, AI agents, etc, **verifiably demonstrating control and authority.**



vLEI Core Functions



Digital signing

Digital sealing or signing (of documents, contracts, reports, invoices, data) by a legal entity or authorized representative



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

ISO 5009 - Official organizational roles — Scheme for official organizational roles

Key provisions of this document include:

- Understanding the official roles of persons acting on behalf of organizations is an important consideration in fulfilling both commercial business and regulatory interactions and obligations.
- Main goals are:
 - providing lists of official organizational roles;
 - leveraging the experience of ISO/TC 68 in defining and maintaining reference data standards;
 - defining an official organizational

Highlights:

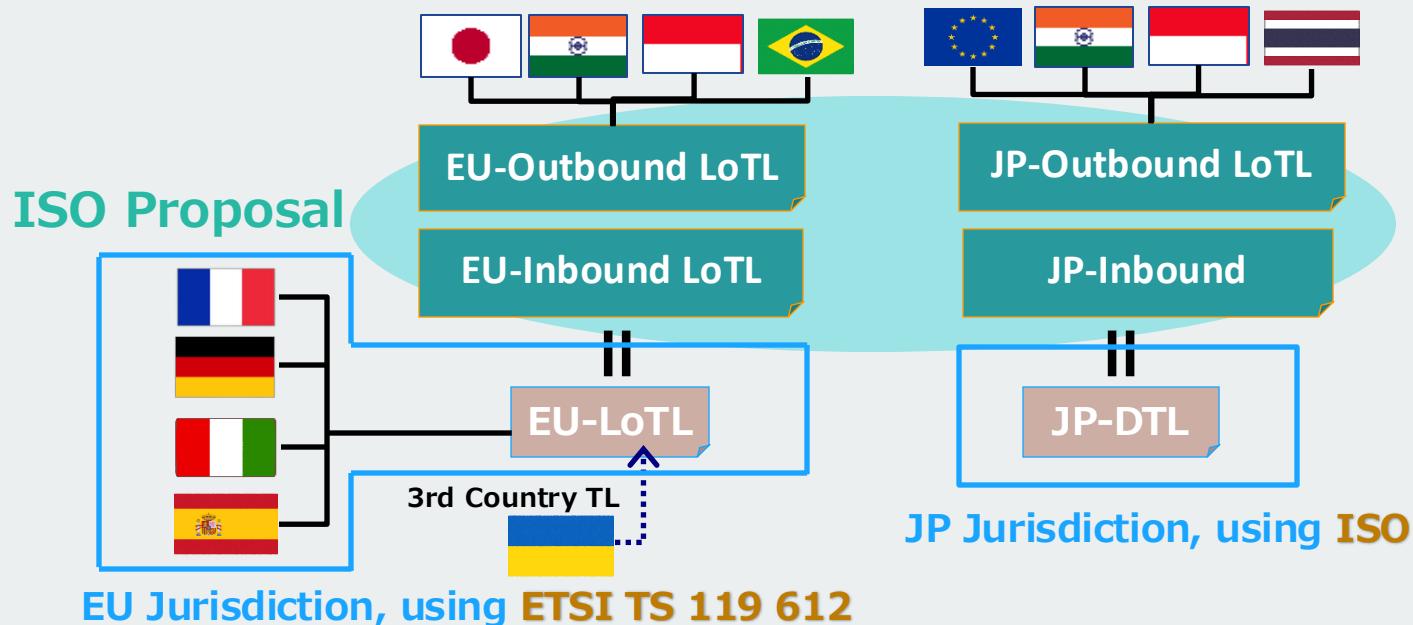
- ISO/TC 68 sees that this document can be used to specify in a standard way the optional role extension contained in X.509 (ISO/IEC 9594-8) public key certificates with embedded LEIs, as outlined in ISO 17442-2.
- This document can also be used to indicate roles in a standard way in digital verifiable credentials, the format for interoperable, cryptographically verifiable digital credentials being defined by the W3C standards organization.
- Combining LEIs with official organizational roles can become a key enabler for digital identity management.
- Further information on the ISO 5009 standard can be found on the [ISO website](#).

Additional comments on ISO 5009....

- **GLEIF is becoming the maintenance agency for it.**
- The development of the ISO 5009 standard was initially proposed by GLEIF to bring clarity and structure to the role information held in both of these LEI-based digital tools.
- As an active participant of ISO/TC 68, **GLEIF led the development work**. The ISO technical management board assigned the Maintenance Agency to the Swiss Association for Standardization (SNV), which passed its responsibilities to GLEIF. Therefore, **GLEIF will remain closely involved in the management of the operations of the ISO 5009 going forwards, as the operational Maintenance Agency for the standard.**



Japan Use Case: Proposal to ISO: Inbound/Outbound



Issues to be considered based on POC results:

1. Mutually recognized countries(Outbond) may vary depending on the country and jurisdiction
2. Regional top-level trust lists (Inbound) should be separated by jurisdiction from a data sovereignty perspective

Proposal to ISO: Trustlist method that separates inbound and outbound

Inbound: A pointer to DTL which is a list of trust services recognized in the jurisdiction

Outbound: A list of pointers to inbound TL (LoTL) of counterparty countries mutually recognized by the TL (LoTL) issuing country under a treaty between countries or regions

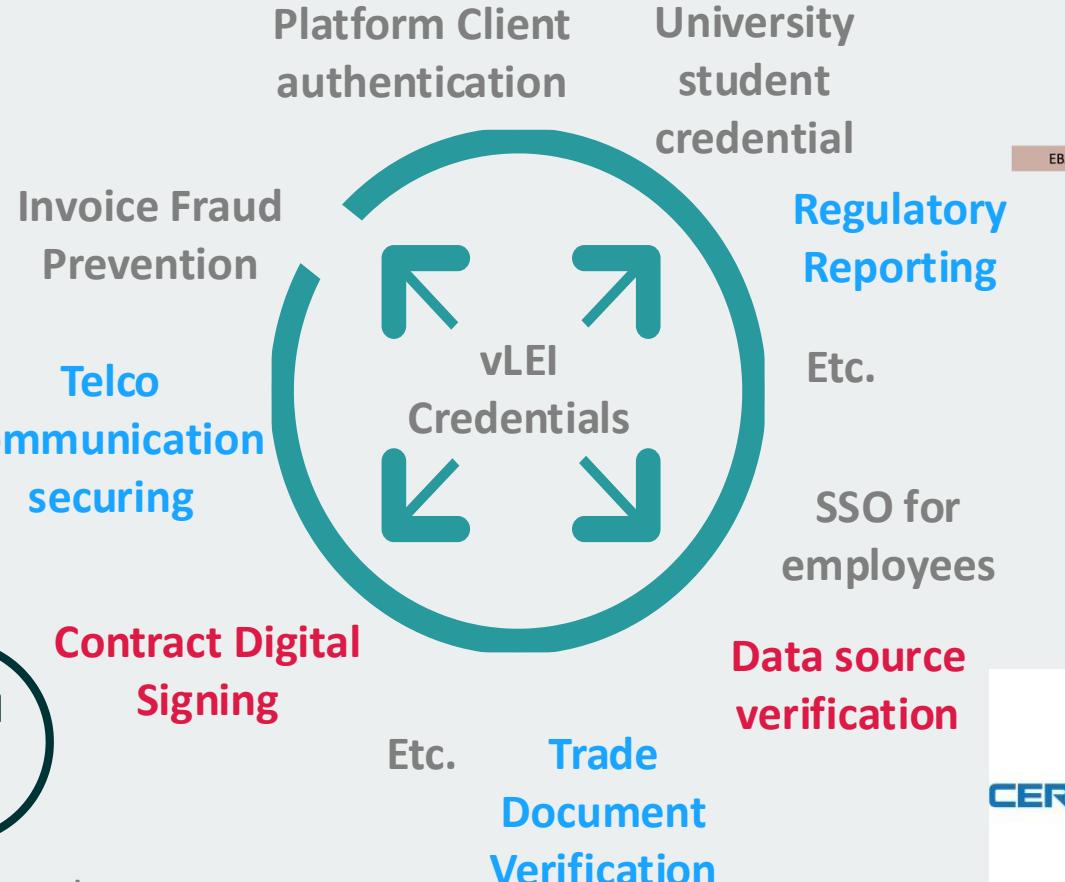
Releasing the Power of Organizational ID

Official Organizational Role (OOR) & Engagement Context Role (ECR) Credentials

GSMA Foundry
Open Verifiable
Calling project



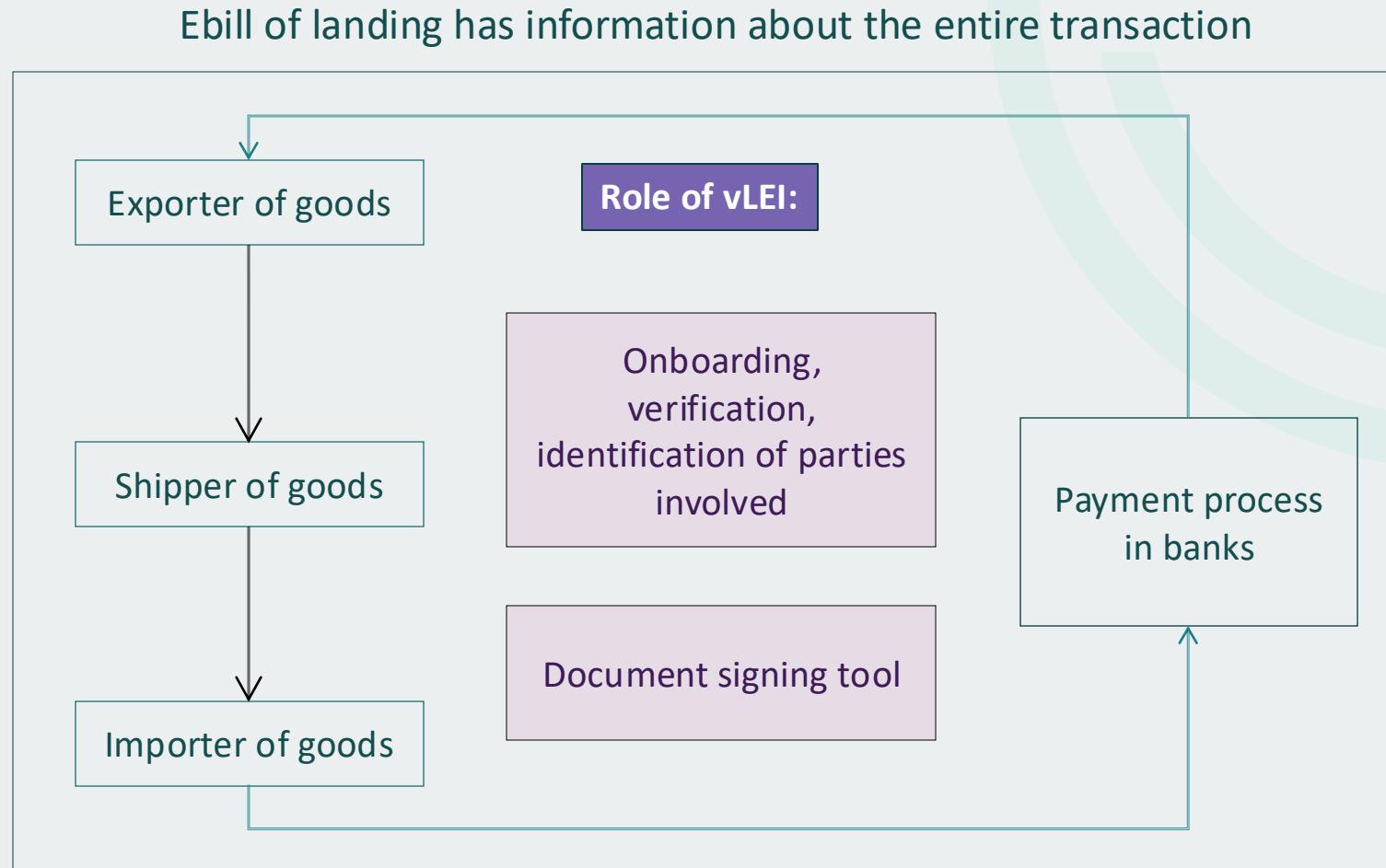
GLEIF Annual
Report 2024



Prudential Disclosures
to EBA via P3DH

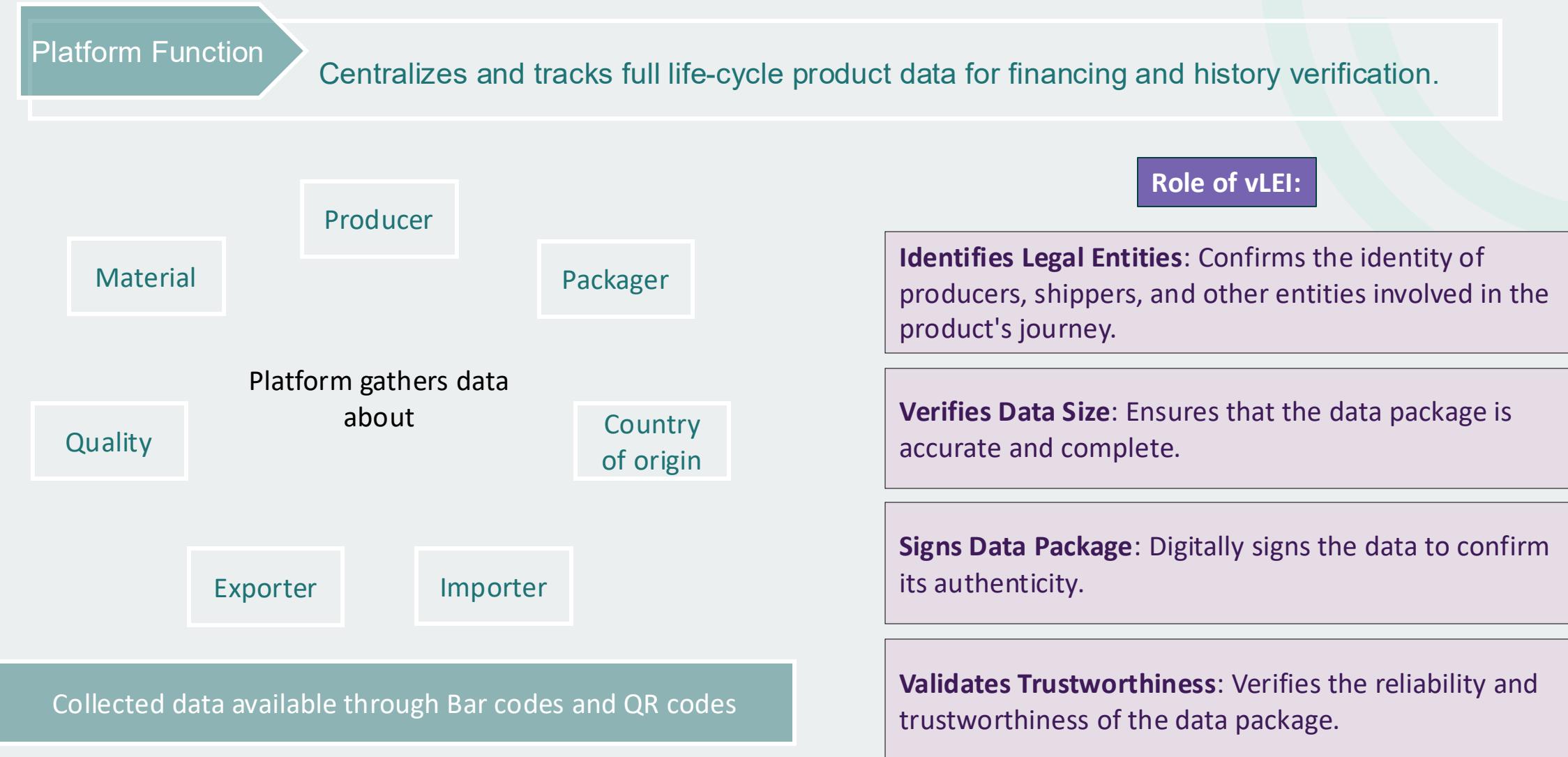


CFCA Use Case: E-bill of Lading in Shanghai Free Trade Zone

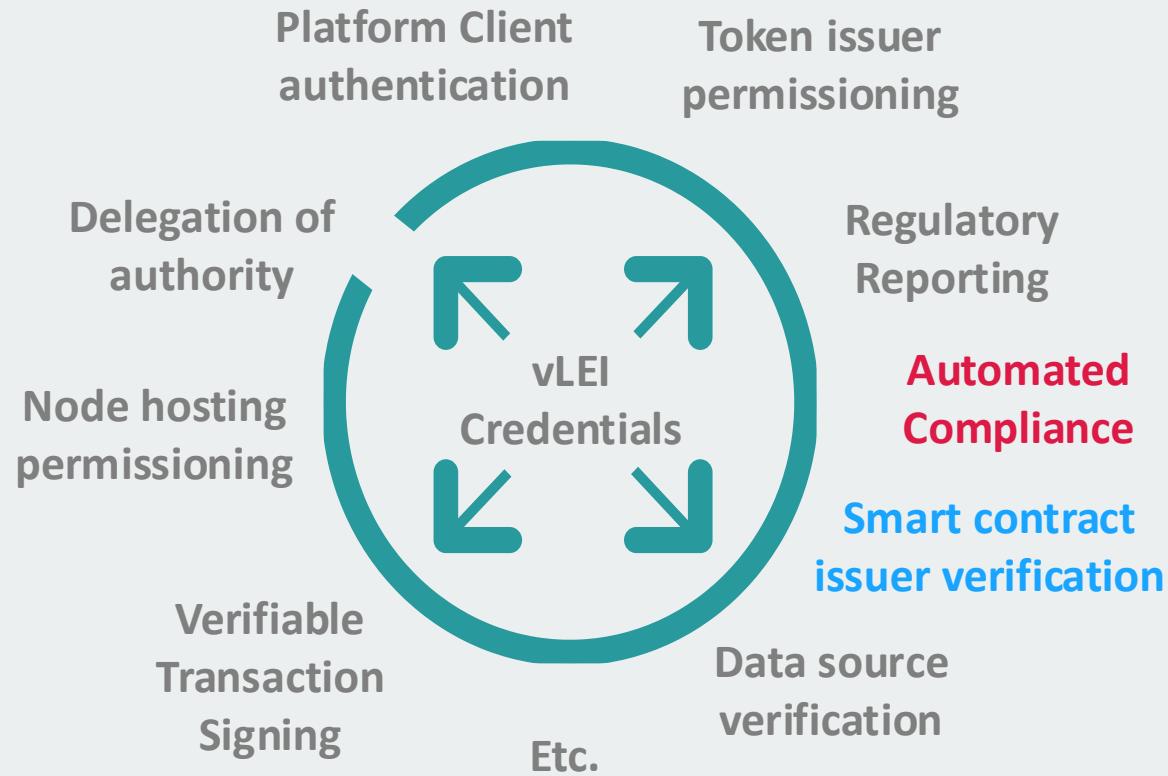


E-bill of Lading in Shanghai Free Trade Zone: Utilizes vLEI to identify enterprises and their employees on a digital trade platform, serving as both a unique identification and an online authentication and document signing tool.

Certizen Use Case: Products Traceability Center



In Blockchain



Conclusion

- GLEIF is a real global organization
- GLEIF enables Product passport, supply chain, SBOM
- Offer for cooperation:
 - ETSI or WebTrust certified CA or TSP can become LOU/QVI easier



*Enabling global identity
Protecting digital trust*



Limitations

- This presentation contains confidential and proprietary information and/or trade secrets of the Global Legal Entity Identifier Foundation (GLEIF) and/or its affiliates, and is not to be published, reproduced, copied, or disclosed without the express written consent of Global Legal Entity Identifier Foundation.
- Global Legal Entity Identifier Foundation, the Global Legal Entity Identifier Foundation logo are service marks of Global Legal Entity Identifier Foundation.