



August 29, 2024

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency,
400 7th Street, SW
Suite 3E-218
Washington, DC 20219

RE: Comments Regarding Proposed Financial Data Transparency Act Joint Standards

Dear Sir or Madam:

I have reviewed the draft proposal for Financial Data Transparency Act Joint Standards and have been invited to comment based on my leadership in the digital governance space and my history in working with US government organizations.

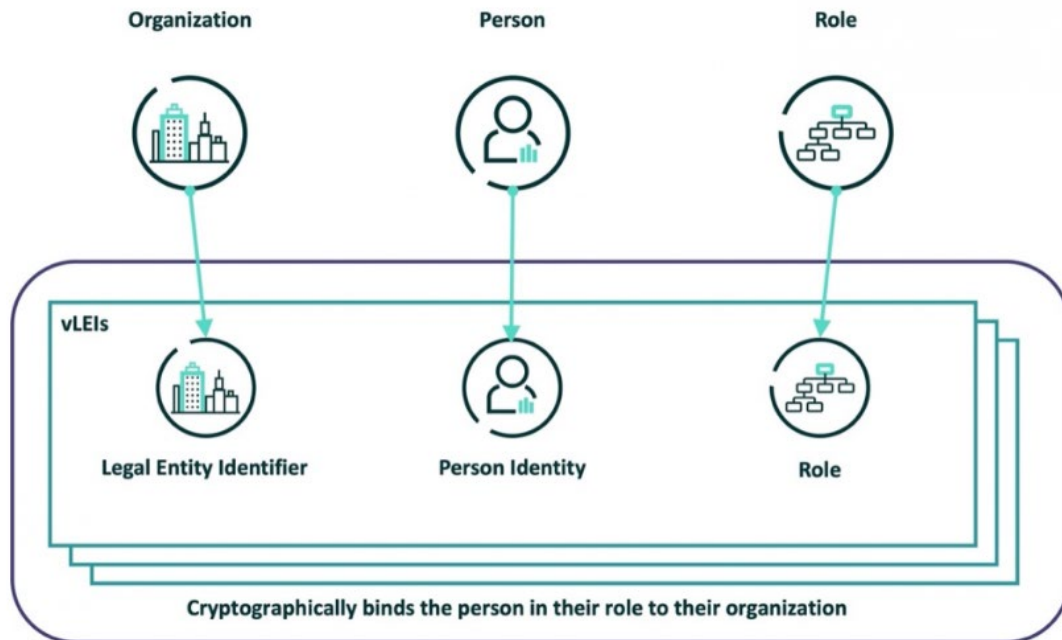
After a career in auditing trust anchors for the US. Federal Public Key Infrastructure and public certification authorities as an authorized WebTrust auditor, I have recently started a consultancy focused on interoperable trust and usage of decentralized digital credentials based on cryptography.

Over the last nine years, we have seen a consistent movement to using cryptography in creating more confidence in the source and content of digital information through the use of verifiable credentials. The technology, and its supported governance, allows individuals and roles to bind cryptographic signatures to digital objects so that relying parties have substantial confidence that the asserted signatories actually signed digital documents and that the digital document has not been tampered with since the signing operation.

While I commend that the proposed act includes the use of Legal Entity Identifier as the legal entity identifier joint standard, the proposal falls short in not mandating the use of a verifiable Legal Entity Identifier (vLEI). A vLEI is a secure digital version of a Legal Entity Identifier (LEI) code. It's a trustworthy digital credential that can be automatically verified without human intervention. The goal of a vLEI is to enable organizations to collaborate and innovate without being limited by geography, money, or other factors. It also allows for the secure and efficient flow of goods, services, and money around the world.

The vLEI is a critical extension of the LEI; Once a vLEI is issued to an Organization, vLEIs can be issued to Persons who represent Organizations either in official or functional roles. In discussions within the US Federal PKI Certificate Policy Working Group, Role certificates are emerging as a requirement for use in authorized and confidence-inducing communication.

By combining three concepts – the organization's identity, represented by the LEI, a person's identity and the role that the person plays for the organization, vLEI credentials can be issued.



vLEI Role Credentials issued to Persons whose **Official Organizational Roles** (ISO 5009 standard) that can be verified both by the organization as well as against one or more public sources, or through official documents obtained from the organization such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person.

Example:

- vLEI Role Credential for a CEO
- Can be used to:
 - carry out official duties and powers conferred legally or required by regulation, e.g., annual reports, regulatory reports
 - carry out internal policies, duties or tasks, e.g., approve strategic plans, sign employee service awards

vLEI Role Credential issued by Legal Entities to Persons **in the context of the engagement** of those Persons with an organization which can be verified by the organization.

Example:

- vLEI Role Credentials issued by an organization to its authorized suppliers
 - Requirements for use defined by the organization
 - Could require authorized suppliers to submit invoices signed with their vLEI Role Credentials to eliminate presentation of fraudulent invoices

The United States is lagging behind other countries in the establishment of verifiable digital identities to promote trust and confidence in assertions made by authorized persons. The European Union has ratified eIDAS 2.0. The purpose of eIDAS 2.0 is to make electronic transactions across EU member states more secure and streamlined, while also increasing trust and interoperability.

Here are some of eIDAS 2.0's objectives:

- **Improve safety and flexibility:** Allow digital identities to be used in a variety of contexts, such as accessing public services, online document signing, and border crossings.



- **Create a European digital identity wallet:** Allow EU citizens to use their digital identity to access commercial and government online services across Europe.
- **Strengthen safeguards around personal information:** Allow users to share their identification through a mobile super app without exposing personal details like their age, address, or birth date.
- **Expand the number of services covered:** Apply the regulation to more services, such as e-certificates for authentication.
- **Make electronic transactions more consistent:** Make it easier to implement electronic transactions, especially through the EUDI Wallet.
- **Make electronic transactions safer and more convenient:** Incorporate safer and more convenient electronic transactions into daily activities like booking flights, filling out rental agreements, and applying for jobs

Any proposed Act that does not mandate the use of this technology will likely lead US government organization further behind in global interoperability, cost saving, and risk/fraud reduction measures that are rapidly becoming available in the marketplace.

Scott S. Perry CPA, CISA
Principal