Governance Framework for Issuer Identity Registries

June 9th, 2025

Prepared by:

Credential Engine
Digital Credentials Consortium

Authors:

Jeanne Kitchens, Chief Technology Services Officer, Credential Engine
Kerri Lemoie, PhD, Director, MIT, Digital Credentials Consortium
Rob Schwartz, Senior Software Engineer (Contract), MIT, Digital Credentials Consortium

Background

This governance framework was developed collaboratively by Credential Engine and the MIT Digital Credentials Consortium (DCC) as part of the *Issuer Identity Registry Research Project*, conducted from May 2024 through June 2025. It reflects input from the project's Advisory Group, which included representatives from standards bodies, state agencies, education and workforce organizations, and technical experts.

The framework is intended to serve as guidance for organizations designing, implementing, or operating issuer identity registries, particularly in the context of decentralized identity and Verifiable Credential (VC) ecosystems. It outlines seven key governance areas essential to establishing trustworthy and transparent registry operations.

Each governance consideration is tagged to indicate its alignment with principles from the Integrative Model of Organizational Trust to help implementers identify how specific policies and structures contribute to building and maintaining trust in a registry and its participants.

More information about the research and design work behind this framework is available in the full ***Issuer Identity Registry Research Report***[1], published by Credential Engine and the Digital Credentials Consortium.

[1] Kitchens, Jeanne; Joy, Rohit; Lemoie, Kerri; Schwartz, R.X.; Walsh, Gillian (2025): *Issuer Identity Registry Research Report: Designing Trust Infrastructure for W3C Verifiable Credentials Being Used for Learning and Employment Records*. Credential Engine and Digital Credentials Consortium. Published June 9th, 2025. Available here.

Table of Contents

Introduction

This document outlines governance areas for issuer identity registries, offering a practical and adaptable governance framework that can be adopted by implementers. It is intended to guide organizations in establishing trusted and transparent governance practices that align with Verifiable Credential (VC) ecosystems and support the interoperability and reliability of credential data.

To support trust in decentralized VC ecosystems, organizations operating issuer identity registries should maintain a publicly accessible webpage that clearly outlines their governance policy. This policy should detail the principles, procedures, oversight, and accountability mechanisms guiding the registry's operation.

Additionally, a reference to this governance policy should be included in the registry metadata, using the policy_uri field as defined in the **OpenID Federation specification**. This link should be associated with information about the organization offering or operating the registry. Details about issuer identity metadata are provided in *Kitchens, Jeanne; Joy, Rohit; Lemoie, Kerri; Schwartz, R.X.; Walsh, Gillian (2025): Issuer Identity Registry Research Report: Designing Trust Infrastructure for W3C Verifiable Credentials Being Used for Learning and Employment Records.* Credential Engine and Digital Credentials Consortium. Published June 9th, 2025. Available here. See the Report's *Issuer Identity Registry Prototypes and Shared Features* section.

Making governance policies easily accessible and linked directly to registry data helps build transparency, supports automated trust evaluation, and strengthens the credibility of issuer identity registries within verifiable credential ecosystems.

Trust Framework Alignment

Because trust is the foundational motivation for using issuer identity registries in VC ecosystems, this framework incorporates a trust-building lens informed by research. Specifically, it draws from the ***Integrative Model of Organizational Trust*** [2], which identifies core characteristics that help establish and maintain trust within organizational contexts.

Each of the governance areas described in the following section includes tags that indicate alignment with this model. These tags—(A), (B), and (I)—signal whether a given item primarily supports principles related to Ability, Benevolence, and Integrity, respectively. These dimensions may apply across different stakeholder groups, including issuers, verifiers, and registry operators.

Ability: "Ability is that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain. The domain of the ability is specific because the trustee may be highly competent in some technical area, affording that person trust on tasks related to that area."[3]

- ***Example:*** *Mechanisms for validating records against the issuer identity registry's cryptographic signature.*

Benevolence: "Benevolence is the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive. Benevolence suggests that the trustee has some specific attachment to the trustor."[4]

- ***Example*****:** Organizational mission.

Integrity: "The relationship between integrity and trust involves the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable. Such issues as the consistency of the party's past actions, credible communications about the trustee from other parties, belief that the trustee has a strong sense of justice, and the extent to which the party's

[2] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335SciSpace+2

[3] Ibid.

[4] Ibid.

actions are congruent with his or her words all affect the degree to which the party is judged to have integrity."[5]

- ***Example:*** *Frequency and criteria for periodic reviews and estimated processing time.*

Issuer Identity Registry Governance Framework

The following governance framework outlines seven core areas essential to the design, operation, and oversight of issuer identity registries. Each area includes specific considerations that contribute to trust and transparency, and they are tagged using the ***Integrative Model of Organizational Trust***:

- (A) for Ability
- (B) for Benevolence
- (I) for Integrity

These tags signal how each governance element contributes to trust-building across stakeholders in Verifiable Credential ecosystems.

[5] Ibid.

1. Registry Overview and Purpose

Defines the scope, objectives, and operational principles of the issuer registry.

- **Purpose and scope of the registry:** Defines the scope and purpose of the registry. (A I)
- **Subject matter focus of the registry:** Limited to issuers, potentially specific types of issuers. (A B I)
- **Funding model and sources:** Description of funding sources for registry operations. (B I)
- **Business model and fee structure for issuers:** Explanation of any fees or costs associated with issuer participation. (A B I)
- **Use/storage of private individuals' data:** Storage of private data should ideally not occur, or should be strictly minimized. (A B I)

2. Governing Parties and Oversight

Addresses the roles and responsibilities of the governing bodies and mechanisms for ensuring transparent, effective oversight of an issuer registry.

- **Organization:** Organizational mission. (B)
- **Governing body or advisory board structure:**
    - Composition and roles. (A B I)
    - Processes for decision-making and resolving disputes. (A B I)
- **Responsibilities of the governing parties:**
    - Oversight of operations, policies, procedures, and performance. (A)
    - Communication and transparency policies for governance decisions. (B)
    - General transparency and accountability to stakeholders. (B I)
- **Dispute resolution mechanisms:** Protocols for handling conflicts or challenges related to registry governance. (A B I)
- **Communication and reporting:** Channels for stakeholder engagement (e.g., messaging about updates to the registry, requests for updates from participants, updates about the organization hosting the registry, and other relevant communications). (A B)

3. Privacy Policy and Terms of Use

Establishes the legal and contractual rights and obligations of the issuer registry with respect to data providers and data users.

- **Liability:** Provisions to hold the issuer registry owner harmless from certain claims or misuse of the registry. (B I)
- **Misuse of data:** Policies and consequences for improper use of registry data. (B I)
- **Privacy and data protection requirements**:
    - Compliance with applicable laws. (B I)
    - Credential holder privacy protections (e.g., preventing "calling home," etc.). (B I)
- **Intellectual property and licensing considerations:** Ownership and usage rights for registry content and data. (B I)

4. Issuer Information and Verification

Details the processes and requirements for onboarding, verifying, and maintaining issuer data.

- **Process for initial issuer data submission:** Mandatory and voluntary issuer information (e.g., name, description, location, identifiers, credentials offered, contact information, etc.). (A I)
- **Process for verifying issuer identity and legitimacy:**
    - Know Your Customer (KYC) process/other identification process. (A I)
    - Use of third-party services (if any). (I)
- **Process for reviewing and maintaining issuer information:**
    - Initial verification steps and estimated processing time. (A I)
    - Frequency and criteria for periodic reviews and estimated processing time. (I)
- **Trust and reputation policies:**
    - Defining trust levels or scales based on criteria met (e.g., evidence-based ratings). (A B I)
    - Addressing negative attestations or endorsements of issuers (e.g., "bad reviews"). (A B I)
- **Issuer planned/emergency key rotation and/or key compromise policies:** Including response, audit, and notification policies. (A I)
- **Retention and archival policies:** Longevity of issuer data for long-term verification. (A I)

- **Policies for organizations that close, merge, or leave the registry:** Defines processes and expectations for handling issuer records when organizations close, merge, or voluntarily leave the registry. (A B I)
- **Good-faith policies for payment defaults or non-renewal:** Describes how the registry will address situations where issuers fail to pay fees or do not renew participation in good faith. (B I)
- **Policies for issuer removal:** Voluntary exit or non-compliance. (B I)
- **Documentation for issuers:** Provides guidance and reference materials to help issuers understand registry requirements, processes, and best practices. (A B I)
- **Issuer support contact:** Provides contact information or support channels for issuers to request assistance or report issues. (A B)

5. Data Download Format

Details the processes and policies regarding downloading issuer registry data.

- **Machine-readable and human-readable issuer registry retrieval methods:** Describes the formats and methods available for retrieving issuer registry data in both machine-readable and human-readable formats. (A I)
- **Public vs. private registry access:** Defines which portions of the registry are publicly accessible and which may require controlled access. (A B I)
- **Documentation for users:** Provides guidance and reference materials to assist users in accessing and utilizing registry data. (A B I)
- **User support contact:** Provides contact information or support channels for users to request assistance or report issues related to registry data access. (A B)

6. Technical Standards

Establishes the technical foundation for an issuer registry based on specific standards used.

- **DID URL/traditional URL/other identifiers used:** Specifies which types of identifiers are used for issuers in the registry (e.g., DID URLs, traditional URLs, other identifiers). (A I)
- **Machine-readable credential formats supported:** Describes the credential formats supported by the registry for interoperability. (A I)
- **Issuer registry standard/standards used:** Identifies the technical standards and protocols implemented in the registry. (A I)
- **Cryptographic signing mechanisms:** Describes how external applications can confirm the integrity of registry records through cryptographic signatures. (A)

- **Verification infrastructure:** Mechanisms for validating records against the issuer's cryptographic signature and the issuer registry's cryptographic signature. (A)
- **Verifier integration guidance**: Provides documentation or guidance on how verifiers can integrate with the registry, access verification endpoints, and consume registry data for trust evaluation. (A B I)
- **Support for tamper-proof storage of records:** Describes methods used to ensure tamper-evident storage of registry records (e.g., append-only logs, blockchain). (A I)

7. Security and Operations

Describes cybersecurity and technical operations information regarding how the issuer registry code is operated and maintained.

- **Security controls and data protection methods:** Describes the security controls, protocols, and practices used to protect registry data and systems. (A B I)
- **Service Level Agreement (SLA) commitments:** Defines the registry's service level expectations, availability, performance guarantees, and response times. (A B I)
- **Issuer registry planned and emergency key rotation and/or key compromise policies:** Describes procedures for planned key rotation and response protocols for key compromise scenarios (including response, audit, and notification policies). (A I)
- **Open-source or closed-source code:** Indicates whether the registry's codebase is open-source or closed-source, and any relevant licensing or transparency practices. (A B I)
- **Existence of production and test environments and automated testing:** Describes whether the registry maintains separate production and test environments, and the use of automated testing to ensure system quality and reliability. (A I)

Re-use and Attribution

When citing this paper, use: Kitchens, Jeanne; Lemoie, Kerri; Schwartz, R.X.; Walsh, Gillian (2025): *Governance Framework for Issuer Identity Registries.* Published June 9th, 2025. Available here.

This document contains content from the research work "Developing A Governance Framework for Learning and Employment Record (LER) Issuer Registries" published in May 2025.[6] Attribution should be made under the Creative Commons Attribution-ShareAlike 4.0 International License. When citing that paper use: Schwartz, R.X.; Lemoie, Kerri; Kitchens, Jeanne (2025): Developing A Governance Framework for Learning and Employment Record (LER) Issuer Registries. Open Identity Summit 2025. DOI: 10.18420/oid2025_03. Bonn: Gesellschaft für Informatik e.V.. PISSN: 2944-7682. pp. 41-54. Regular Research Papers. Neubiberg, Germany. 22.-23. May 2025.

Acknowledgements

We extend our sincere gratitude to Walmart for their generous support, which made the Issuer Identity Registry research project possible.

We also thank the members of the Issuer Registry Advisory Group, whose expertise and guidance were instrumental in shaping the project's direction.

Our appreciation goes to the stakeholders from education, workforce, and technology sectors who participated in outreach and engagement efforts, providing valuable feedback that enriched our understanding and informed our recommendations.

Finally, we acknowledge the broader community of practitioners, policymakers, and advocates working towards secure, interoperable, and user-centric digital credentialing systems.

[6] Schwartz, R.X.; Lemoie, Kerri; Kitchens, Jeanne (2025): Developing A Governance Framework for Learning and Employment Record (LER) Issuer Registries. Open Identity Summit 2025. DOI: 10.18420/oid2025_03. Bonn: Gesellschaft für Informatik e.V.. PISSN: 2944-7682. pp. 41-54. Regular Research Papers. Neubiberg, Germany. 22.-23. May 2025