Credential Engine and Digital Credentials Consortium: Issuer Identity Registry Research Report

Designing Trust Infrastructure for W3C Verifiable Credentials Being Used for Learning and Employment Records

June 9th, 2025

Prepared by:

Credential Engine
Digital Credentials Consortium

Authors:

Jeanne Kitchens, Chief Technology Services Officer, Credential Engine
Rohit Joy, Director of Engineering, Credential Engine
Kerri Lemoie, PhD, Director, MIT, Digital Credentials Consortium
R.X. Schwartz, Senior Software Engineer (Contract), MIT, Digital Credentials Consortium
Gillian Walsh, Operations and Project Manager, Digital Credentials Consortium

Description:

This report documents a joint research effort by Credential Engine and the Digital Credentials Consortium to explore, design, and test issuer identity registries—digital, structured directories that confirm the legitimacy of organizations authorized to issue credentials. These registries do not issue credentials themselves. Instead, they provide a foundational layer of trust for verifying the identity of credential issuers in ecosystems that use verifiable credentials, such as Learning and Employment Records (LERs).

Re-use and Attribution:

When citing this paper, use: 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

Executive Summary

In an increasingly digital world, issuing digital credentials is essential to ensure that every learner has access to a record of their achievements. Learning and Employment Records (LERs) issued in alignment with the World Wide Web Consortium Verifiable Credentials (W3C VC) specification, including Open Badges 3.0 and Comprehensive Learner Record 2.0, help to assure that the digital credentials are secure, privacy-enhanced, portable, and independently accessible records of achievements. Digital credentials issued in these standards are digitally signed by the issuer and are therefore tamper-evident, machine-verifiable, and persistently accessible to learners, without dependence on the issuing organization to store or manage ongoing access to the data.

However, cryptographic integrity alone does not establish trust. For W3C VC ecosystems to function effectively, stakeholders must be able to trust not only the credential but also the legitimacy of the issuer's identity. This trust must be built into the ecosystem's architecture. A critical component of this infrastructure is the issuer identity registry: a machine-readable, structured data service that confirms whether the identity of an issuing organization has been validated by a known and trusted entity. Issuer registries are not used to issue credentials. Instead, they provide a trust layer that associates an organization's digital identifier directly to the verifiable credentials that organization issues.

While issuer registries are a critical aspect of all W3C VC ecosystems, LERs have unique needs. This project focuses on that context specifically and in particular, on the identity of the issuer. In the future, LER registries may also encompass accreditation, qualifications, and known credentials in addition to the identity of the issuer. The aim of this project has been to establish a foundational layer of trust, validating issuer identity, so that LER ecosystems will have recommendations to build upon.

This report outlines the joint research initiative by Credential Engine and the Digital Credentials Consortium from May 2024 to June 2025, which includes the issuer identity registry and specifications analysis, governance evaluation, development of two issuer

identity registry prototypes and open-source software, all grounded in open standards and transparent collaborative practices.

The report highlights the importance of using interoperable specifications and explores how issuer registries support trusted verification processes while respecting privacy and decentralization.

This work would not have been possible without the generous support of Walmart, whose sponsorship enabled this cross-sector collaboration to move from concept to proof of implementation. Their investment reflects a broader commitment to empowering individuals with verifiable records that improve access to learning and employment opportunities across dynamic global ecosystems.

Credential Engine / DCC Issuer Identity Registry Research Project

From May 2024 to June 2025, Credential Engine and the Digital Credentials Consortium (DCC) collaborated to explore the governance and technological requirements for implementing issuer registries within education and workforce W3C Verifiable Credentials ecosystems. This joint research focused on developing interoperable, specifications-based infrastructure to enhance trust in digital credentials by enabling verifiers to confirm the legitimacy of credential issuers across various systems.

The project resulted in the following key deliverables:

- **Issuer Identity Registry Advisory Group**: A chartered group of subject matter and technical experts convened to define the advisory group's charter, generate use cases, identify governance criteria, and contribute to the development of issuer identity registry prototypes.

- **Research on Governance and Specifications**: Conducted systematic and methodologically sound research focusing on both the governance structures and technical specifications necessary for effective issuer identity registry implementation.

- **Issuer Identity Registry Prototype Development and Testing**: Both Credential Engine and DCC developed, hosted, and tested issuer identity registries. Both issuer registries used the same metadata and API endpoint specifications described in this report. Both prototypes underwent testing to assess functionality and interoperability.

- **Educational Outreach and Community Engagement**: Creation of blogs and presentations aimed at explaining issuer identity registry-related topics to engage a broad audience, fostering understanding. Encouraged other organizations to explore and implement issuer or verifier registries, promoting widespread adoption and collaboration.

- **Comprehensive Applied Research Report**: Compiled this report encapsulating research findings, prototype specifications, governance considerations, and recommendations for future implementations.

This project established a robust framework for issuer identity registries, enhancing the integrity and trustworthiness of verifiable credentials within diverse educational and professional ecosystems.

Issuer Identity Registry Project Team

Credential Engine and the DCC collaborated to explore the governance and technological requirements for implementing issuer registries within verifiable credential ecosystems. This joint initiative focused on developing interoperable, standards-based infrastructure to enhance trust in digital credentials by enabling verifiers to confirm the legitimacy of credential issuers across various systems.

Credential Engine

Credential Engine is a nonprofit organization dedicated to increasing transparency and accessibility in credentialing. It maintains both the Credential Registry—a cloud-based platform housing structured data on a wide array of credentials and credential issuers—and the Credential Transparency Description Language (CTDL), a standardized, machine-readable framework that enables transparency, discoverability, and interoperability across systems.

CTDL defines credential types and provides a comprehensive set of properties—such as requirements, learning outcomes, skills, and assessment methods—that allow organizations to describe credentials in a consistent and semantically meaningful way. This structure ensures that every component of a credential description can be accurately interpreted and reliably reused by digital systems.

The structured format of CTDL supports comparability, integration, and trusted credential data discovery and exchange across diverse education and workforce ecosystems. It is actively utilized in Learning and Employment Records (LERs), counseling platforms, career navigation tools, and pathway resources. While CTDL has been adopted by most U.S. states, it is designed for global applicability and can be adapted for use in various national, regional, and institutional contexts.

Credential Engine develops and maintains both CTDL and the Credential Registry to support its mission of enhancing credential transparency. It upholds governance policies and operational processes that promote data quality and interoperability. These efforts provided a strong foundation for the issuer identity registry research project conducted in collaboration with the DCC, informing plans to integrate issuer identity registries as a core component of scalable, trustworthy verifiable credential ecosystems.

The Digital Credentials Consortium

The Digital Credentials Consortium (DCC) is a global network of postsecondary education institutions collaborating to advance the understanding and use of privacy-enhanced, portable, verifiable digital credentials through open source technology development and leadership, research, and advocacy. DCC's member-based community is governed by a Leadership Council which provides strategic direction for the consortium as it aims to provide solutions that empower learners and institutions alike.

Since its inception in 2018, the DCC has developed and implemented a suite of open source software for issuing, sharing, and verifying World Wide Web Consortium Verifiable Credentials (W3C VCs) and related standards for education and training, including Open Badges 3.0 (OBv3). The DCC software stack includes customizable issuer microservices for issuing W3C VCs that can be implemented alongside existing student information systems and learning management

platforms. Institutions can choose to leverage individual microservices as needed or install the DCC admin frontend dashboard, which allows for simple issuing in batches with CSV file upload. Additionally, the DCC hosts VerifierPlus, a website that allows a verifier (such as an employer or academic institution) to check the authenticity of a credential.

The DCC developed the specification and code base for the open source Learner Credential Wallet (LCW), a mobile platform for iOS and Android that enables learners to claim, store, and share W3C VCs. In 2024, stewardship of the LCW was transferred to the Open Wallet Foundation, though the DCC maintains leadership in development of the wallet's features and functionality. The research-informed development and implementation of issuer registries as documented in this report adds significant value to DCC software and W3C VC technology for credential ecosystems, providing an additional layer of trust.

Establishing Trust in W3C Verifiable Credential Ecosystems

This report centers on the development and implementation of issuer identity registries as foundational components for trust in W3C VC ecosystems.[1] While these registries are crucial for validating the identity of credential issuers, the role of verifiers is equally essential to complete the trust loop. Verifiers—entities that assess and verify credentials—must effectively utilize issuer identity registries to streamline their processes, ensuring that credentials are both authentic and issued by recognized organizations.

In W3C VC ecosystems, establishing the legitimacy of credential issuers is paramount. While W3C VCs provide cryptographic assurance of data integrity and authenticity, they do not specify how human sourced validity of the issuer should be performed. This gap can lead to challenges such as:

- **Impersonation and Fraud**: Malicious actors might issue counterfeit credentials, falsely claiming association with reputable institutions. Without a mechanism to verify issuer identities, such fraudulent activities can undermine the credibility of genuine credentials.

[1] Some text in this section sourced from Issuer Registries: Establishing Trust, Privacy, and Efficiency inVerifying Credential Issuers

- **Lack of Standardized Verification**: Inconsistent methods for validating issuer identity can result in inefficiencies and errors, especially when credentials cross institutional or jurisdictional boundaries.

- **Privacy Concerns**: Directly contacting issuers for verification can compromise credential holder privacy, revealing unnecessary personal information and creating potential data security risks.

Issuer identity registries address these challenges by providing architectures to identify organizations recognized as valid issuers of credentials. They support verifiers, credential holders, and systems in substantiating an issuer's identity without compromising privacy. As credentials increasingly traverse platforms, sectors, and borders, these registries—developed in alignment with shared specifications and governance expectations—provide a foundational layer of trust for verifiable credentialing systems. They enable stakeholders to verify the authenticity of credentials and their issuers efficiently, fostering confidence in digital interactions across various domains.

This report does not advocate for a singular, centralized solution. Instead, it acknowledges that multiple registries may exist to serve different communities, jurisdictions, and use cases and that they can take various technical forms—from decentralized implementations using cryptographic keys to registry services managed by networks or institutions. Verifiers may choose to rely on one or more registries based on their specific needs. The project emphasized that issuer identity registries should be built on open, interoperable specifications and supported by clear, accessible governance frameworks, ensuring that registries can scale, interoperate, and maintain trust across diverse ecosystems.

This report is intended to be beneficial to all W3C VC implementations. However, this project focused on how issuer identity registries can be applied in learning and employment ecosystems. Use cases, returned metadata, prototypes, and app interactions in this project were based on this context.

Introduction to Verifiable Credentials

In today's digital landscape, credentials—whether referred to as digital badges, digital credentials, LERs, or other terms—are increasingly issued in digital formats that support privacy and portability. This report focuses on digital credentials that conform to open standards designed for cryptographic verifiability and interoperability. Throughout this report, we use the term W3C Verifiable Credentials (W3C VC) to describe credentials that follow the Worldwide Web Consortium's Verifiable Credentials specification or compatible specifications such as Open Badges 3.0 (OB v3) and Comprehensive Learner Record 2.0 (CLR v2).

A W3C VC is a digital assertion—such as a degree, license, or certificate—that is cryptographically signed, tamper-evident, and machine-verifiable. Credentials issued in this format allow individuals, institutions, and systems to verify the authenticity of the information without contacting the issuer directly, thus ensuring that the credential is shared privately avoiding the potential for tracking.

Within a W3C VC ecosystem, trust is established through the interaction of three core roles:

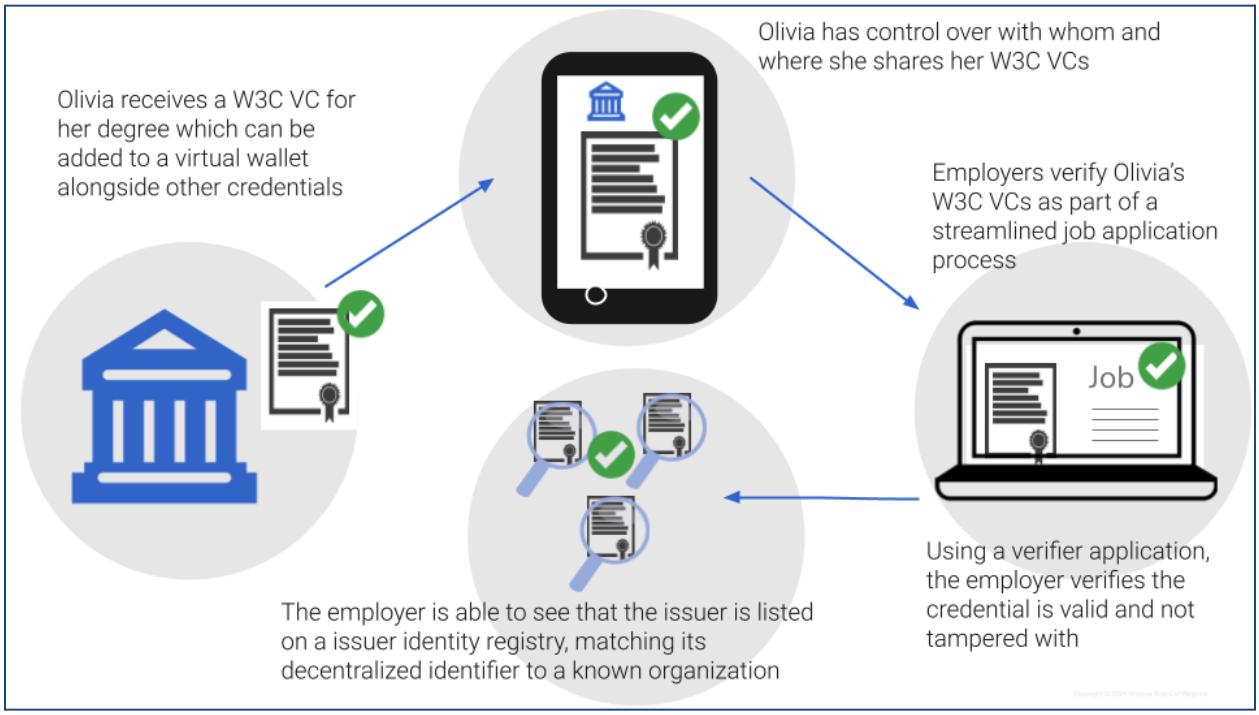
- **Holder:** The individual or entity about whom the credential is issued. For example, a graduate who has earned a Bachelor's degree.

- **Issuer:** The organization or entity that signs and issues the credential, such as a college, university, occupational licensing board, or training provider. Note: The term "issuer" can also refer to the software used to sign and issue a verifiable credential.

- **Verifier:** The individual or entity that seeks to confirm the validity of the credential, ensuring it is authentic, untampered-with, and active (e.g., not revoked or expired). Verifiers may also consult an issuer identity registry to determine whether the issuer of the credential is recognized and trustworthy. Note: The term “verifier” can also refer to software that machine-validates credential and issuer data.

Figure 1 below illustrates the typical flow of a verifiable credential from issuance to the holder, then to a verifier, who queries the issuer identity registry to confirm the issuer’s authenticity.

Figure 1: W3C Verifiable Credentials Data Flow



Attributes of Verifiable Credentials

W3C VCs possess specific attributes that distinguish them from traditional credentials, enabling secure, interoperable, and user-centric digital identity solutions.

- **Cryptographic Integrity**: Each W3C VC is digitally signed by its issuer, ensuring that any alteration to the credential after issuance can be detected. This cryptographic proof allows verifiers to confirm the credential's authenticity without relying on the issuer.

- **Sharable Based on Holder Needs**: W3C VCs are designed for the holder's control, typically stored in a secure digital wallet. Holders can decide when, how, and with whom to share their credentials, without the issuer's permission or involvement.

- **Privacy Preservation**: Because W3C VCs can be shared and verified without contacting the issuer, they can be used without tracking. This is distinct from other types of digital credentials which rely heavily on web-hosted, trackable data. W3C VCs can also support *selective disclosure*, allowing holders to share only the necessary information for a given interaction. This minimizes unnecessary data exposure and enhances privacy.

- **Interoperability and Portability**: Because W3C VCs use open web standards, they can be used across different platforms and systems, facilitating seamless verification across various contexts and jurisdictions.

- **Structured, Machine-Readable Data**: W3C VCs encapsulate detailed information in a structured format, enabling automated processing and integration into digital systems for verification and decision-making purposes.

Benefits of Verifiable Credentials

W3C VCs offer significant advantages across learn and work ecosystems that require secure and efficient data exchange. Their inherent features—such as portability, privacy, interoperability, and structured data—make them particularly valuable in today's digital landscape.

In governmental contexts, W3C VCs are employed for documents like digital driver's licenses and vaccination records, enhancing the security and verifiability of such credentials. Similarly, industries like healthcare, manufacturing, and finance utilize W3C VCs for professional licensures and certifications for specialized skills, ensuring that qualifications are easily verifiable and tamper-resistant.

This report focuses on the application of W3C VCs within LER ecosystems. In these settings, W3C VCs represent micro-credentials, course completions, degrees, certifications, and other forms of learning or training recognition. By using an open standard, W3C VCs provide a scalable solution to issue, share, and verify achievements, thereby supporting mobility, transparency, and trust across interconnected systems of education and employment.

Introduction to Issuer Identity Registries

In W3C VC ecosystems, trust must be intentionally incorporated into the infrastructure. While W3C VCs are cryptographically secure and privacy-preserving, they do not by themselves establish trust in the issuer. Verifiers need a way to confirm that the organization claiming to issue a credential is legitimate and recognized. This is the role of an issuer identity registry.

For credentials issued using open standards such as W3C VCs and OBv3, these registries significantly enhance trust by providing a structured, machine-readable framework for verifying

the source of tamper-evident credentials. They serve as intermediaries of trust by enabling verifiers to confirm issuer identities without contacting the issuer or revealing the verification request—protecting holder privacy and supporting decentralized, user-controlled sharing.

An issuer identity registry is a machine-readable digital service that publishes structured data about organizations that digitally sign and issue W3C VCs. It does not issue credentials or verify their contents. Instead, it serves as a trust layer for verifying issuer identity, helping verifiers determine whether an organization is known, governed, and trusted within one or more ecosystems.

The core of each registry record implemented in this project is the issuer's Decentralized Identifier (DID)—a cryptographically verifiable identifier embedded in the credential itself. The registry lists and exposes these DIDs along with associated metadata such as the issuer's name, public keys, website, contact information, and additional identifiers.

The registry owner—the entity that operates and signs the registry—is the trust anchor in this model. When verifier software queries the registry, it retrieves issuer data that has been digitally signed by the registry owner, ensuring authenticity and data integrity. Verifiers trust the registry because they trust the registry owner's governance model, key management, and data curation policies. A registry owner may be a national body, sectoral alliance, higher education network, or another designated steward.

Issuer identity registries offer significant value by replacing static or siloed methods of listing issuers—such as PDFs, web pages, or private databases—with dynamic, interoperable infrastructure. This enables secure, rapid, and consistent verification of credential issuers across systems, platforms, and jurisdictions. They help reduce fraud, streamline verification processes, and support privacy-preserving architectures.

Application Across Learn and Work Ecosystems

Issuer identity registries have a wide range of applications across multiple sectors:

- **Higher Education**: Institutions can be publicly listed as recognized issuers of degrees, certificates, and micro-credentials—often based on accreditation or regulatory

oversight—improving trust and recognition by employers, credential evaluators, and academic institutions.

- **Certification Bodies and Training Providers**: These entities can be validated as authorized issuers of credentials such as industry certifications, continuing education units, or licenses—including areas like healthcare, skilled trades, and public safety.

- **Government Agencies**: Agencies that issue occupational licenses—such as those in healthcare, education, or skilled trades—can be listed as recognized credential issuers. Governments can also operate issuer identity registries to validate public or private organizations authorized to issue credentials within their jurisdiction, supporting trust and interoperability across regional or national systems.

- **Employers and Verifiers**: Organizations can use issuer registries to confirm that credentials submitted by applicants were issued by trusted, verifiable organizations—reducing fraud and speeding up hiring and admissions processes.

These diverse applications underscore the integral role of issuer identity registries in establishing trust and facilitating efficient credential verification across various sectors within LER ecosystems. If an issuing organization is listed in a governed registry, verifiers can confidently confirm that it is a recognized entity. This capability is especially useful in time-sensitive and risk-sensitive scenarios like job offers, where manual credential checks could delay hiring decisions or expose organizations to fraud.

For credential holders, registry-backed verification ensures that their legitimate achievements are trusted. For employers and other verifiers, it provides an efficient, standards-based way to substantiate issuer identity—reducing administrative burden and the risk of acting on inaccurate or fraudulent claims.

Role of Verifiers in Verifiable Credential Ecosystems

Verifiers are entities such as employers, educational institutions, or government agencies that request and validate credentials presented by holders. Their primary function is to confirm the authenticity and integrity of a credential and to assess the trustworthiness of its issuer.

Verifier software applications utilize issuer identity registries to determine whether a credential originates from a recognized and authorized issuer. When credentials include Verifiable Credential Data Integrity proofs, this process involves checking the issuer's DID against a trusted registry to ensure that the credential has been digitally signed by a verified source.

By relying on issuer identity registries, verifiers can automate and streamline credential validation, reducing the need for manual checks and direct outreach to issuing organizations. This approach enhances efficiency, maintains privacy for both the holder and verifier, and supports scalable trust across sectors and jurisdictions.

Empowering Credential Holders

In verifiable credential ecosystems, the holder, the person about whom the credential is issued, is not just a passive participant, but the central figure. Whether a credential is earned through a university, employer, licensing agency, or another type of provider, it represents real learning, effort, and progress along a person's education and career pathway. People who earn credentials deserve the freedom and trust to use them confidently, without compromising their privacy or facing unnecessary barriers.

W3C VCs support this by enabling credentials to be shared securely, privately, and on the holder's terms. But even more powerful is what becomes possible when issuer identity registries are part of the verification infrastructure. These registries provide verifiers—such as employers or academic institutions—with a structured way to confirm that a credential came from a legitimate source, without contacting the issuer directly or requesting personal information from the holder.

This protects the holder's privacy and speeds up verification. The process is seamless and secure: verifiers can instantly check whether the credential was issued by a recognized, trusted organization. For the person holding the credential, this means their achievements are more likely to be believed and respected. It increases trust in their skills and abilities, especially in settings where trust and authenticity are critical—like job applications, admissions, or licensure.

Issuer identity registries enable a more efficient, transparent ecosystem where people can confidently share their credentials knowing they will be perceived as authentic. This builds a

foundation of trust that supports not only systems and institutions, but the individuals at the heart of those systems—people striving to access opportunities, contribute their talents, and move forward.

Research Question and Focus

Each sector or industry leveraging W3C VC technology has its own set of priorities or challenges when it comes to establishing credential authenticity. Education and employment credentials have complex and unique needs because they have widespread impact across industries, institutions, and borders. This project focused specifically on one foundational aspect of trust: verifying the identity of the credential issuer. It did not address topics such as accreditation status or credential classification, although the research may inform those areas in future work. In earlier digital credential systems—such as web-hosted badges—trust in the issuer often depended on the platform. For instance, a badging platform might have allowed "ABC University" to issue credentials, and users trusted that the platform had verified the institution's legitimacy. This trust was inferred through mechanisms like SSL certificates and platform oversight.

In contrast, W3C VCs are decentralized and individually held by learners. Because these credentials are not tied to a single issuing platform, there is no built-in way for verifiers to know whether the entity listed as the issuer has actually been validated. While VCs include cryptographic features like digital signatures and DIDs, these elements confirm only that the credential hasn't been tampered with—not that the issuer has been verified by a trusted entity.

This raised a core research question for the project:

What mechanisms are needed to reliably confirm that a W3C Verifiable Credential was issued by a legitimate, known organization?

This led to related questions:

- Can issuer identity registries fill this trust gap while preserving privacy and interoperability?
- What governance and technical frameworks are necessary to support such registries?
- How can existing standards and identifiers be used to support scalable solutions?

The project hypothesized that issuer identity registries—designed using open standards and backed by clear governance—could meet these needs. The following section describes how this hypothesis was explored through collaborative research, stakeholder engagement, and the development of working prototypes.

Research and Findings

The project team undertook a collaborative and iterative research process to better understand what contributes to trust in issuer identities and the trustworthiness of the registries that support them. This work focused on both technical infrastructure and governance frameworks necessary for scalable, interoperable, and privacy-preserving trust ecosystems. The research activities included:

- **Advisory group engagement:** A diverse advisory group to generate use cases, identify governance criteria, and contribute to the development of issuer identity registry prototypes.
- **Evaluating specifications**: Multiple existing and emerging specifications for the issuer identity registry were reviewed to select an approach that supports scalability, interoperability, and alignment with current and future needs.
- **Outlining a governance framework**: A structured set of governance considerations were documented affecting trust, usability, and long-term sustainability.
- **Prototyping governance documentation:** Governance structures and responsibilities were implemented by DCC to test how operational transparency impacts trust.
- **Prototyping issuer registries:** Credential Engine and DCC each developed and tested registry prototypes using shared metadata models and technical endpoints.
- **Adapting open-source applications:** DCC modified libraries and applications to interact with the issuer identity registry prototypes.

Advisory Group Engagement

To guide and inform this work, Credential Engine and the DCC convened an advisory group, which was open to all interested participants—including subject matter experts, aspiring experts, users, and technical contributors. The group met regularly to provide input on governance and

technical requirements for issuer identity registries, including use cases, data models, trust attributes, and interoperability needs. Their contributions helped shape the project's approach to building trust infrastructure for verifiable credential ecosystems.

Advisory Group Key Aspects:

- **Composition:** The group included subject matter experts, aspiring experts, credential issuers and verifiers, and technical contributors from education, workforce, policy, government, research, and industry sectors.
- **Objectives:** Members helped define the group's charter, generate use cases, identify governance criteria, inform prototype development, and advise implementers and decision-makers.
- **Scope:** In-scope activities included advising on governance models, data models, specifications, and contributing to prototype development. Out-of-scope topics included commercial use, internal operations of the convening organizations, and product-specific discussions.
- **Engagement:** Scheduled, approximately monthly virtual meetings were held from September 2024 through May 2025, with shared recordings and documents. Participants also contributed asynchronously using collaborative tools.

The group's work shaped use cases, informed the selection of specifications, and guided the development of governance criteria and registry prototypes. All deliverables were released under open licenses to support reuse and broad community benefit.

A full archive of meeting materials and resources, including the charter, recordings, slide decks, and documentation, is linked in the appendix section: Advisory Group Documentation and Resources.

Specification Selection and Evaluation

The project team conducted a comprehensive evaluation of over thirty-five specifications (Appendix: List of Registries and Specifications Evaluated) and implementations to identify those

most suitable for implementing issuer identity registries supporting W3C VC ecosystems.[2] The objective was to select and/or refine specifications that align with modern data standards, support interoperability, and enhance trust between issuers and verifiers. After eliminating inapplicable options, the remaining standards were evaluated using a shared template (Appendix: Specification Implementation and Evaluation Template).

Evaluation criteria included:

- **Open licensing and extensibility:** Ensuring the specification is freely accessible under an open license and extensible.
- **Alignment with modern standards:** It incorporates or builds on up-to-date technical standards.
- **Implementation simplicity:** Ease of implementation and testing for a minimum viable product.
- **Adoption:** Presence of a robust user base or pilot implementations.
- **Support for URLs and DIDs:** Flexibility in accommodating both URLs and DIDs.
- **Governance support**: Accommodates or encourages the development of clear governance policies for registry participation and management.

Based on this evaluation, three key specifications were selected for final evaluation by the DCC and Credential Engine issuer registries: OpenID Federation 1.0, W3C Verifiable Issuers and Verifiers v0.1, (v0.2 was published after research was completed), and DIF Credential Trust Establishment 1.0. Finally the OpenID Federation 1.0 issuer registry standard was selected, along with DID and CTDL standards.

1. Open ID Federation 1.0: The OpenID Federation 1.0 specification was chosen for issuer identity registry implementation. This specification supports federated trust registries, standardized and cascading governance structures, offline caching, strongly opinionated interoperability, and URLs as entity identifiers. The specification is already in use by national governments including Italy, Sweden, and Australia, and is currently in development or being piloted by other implementers like eduGAIN and Germany EUDI Wallet.

[2] Some text in this section sourced from Selecting the OpenID Federation specification for the DCC and Credential Engine Issuer Registry Project | by R.X. Schwartz

It is important to note that OpenID Federation 1.0 uses URLs as entity identifiers and does not natively support DIDs. This may pose limitations for systems that rely on DIDs for decentralized identity management. However, the specification is extensible, and profiles could be developed to support DIDs in the future. By selecting OpenID Federation and exploring ways to align it with DID-based systems, this project contributes to bridging existing web-based trust models with decentralized credential ecosystems.

For reference, the most important parts of the specification used in this project are:

- 3. Entity Statement
- 5.1.1. Federation Entity
- 8. Federation Endpoints

2. Decentralized Identifiers (DIDs): DIDS were selected as the preferred approach for representing entities in the issuer identity registries, aligning with W3C VCs, Verifiable Credential Data Integrity 1.0, and OBv3 specifications. Designed for decentralized, self-managed identity, DIDs provide a secure way to authenticate issuers and holders without relying on centralized authorities. They enhance privacy, user control, and data portability.

A DID is a URI (a unique string of characters) that allows the entity controlling it to prove ownership using cryptographic keys. For example, a DID can look like this:

DID:example:0e036ff07c4cc498e21862873a16fd

This identifier acts as a reference to additional information that the issuer controls. The issuer uses a private key associated with this DID to digitally sign verifiable credentials. Verifiers can then use the corresponding public key to confirm that the credential was indeed issued by the entity that controls the DID.

This project focused on two DID methods—DID:web and DID:key, which are widely adopted in VC ecosystems, including by the DCC.

- **DID:web** encodes the DID into a URL format. For example, did:web:w3c-ccg.github.io resolves to the URL https://w3c-ccg.github.io/.well-known/did.json, where a document is hosted containing public keys.
- **DID:key** embeds a public key directly into the DID itself. It allows immediate verification of the credential's signature.

3. Credential Transparency Description Language (CTDL): CTDL is an open schema maintained by Credential Engine for describing credentials, organizations, learning opportunities, skills, assessments, quality assurance, occupations, and more in a consistent, machine-readable format. Built on linked open data principles, CTDL supports interoperability by structuring and connecting information across systems, enabling data to be discovered, reused, and trusted.

Whereas issuer identity registries provide compact, verifiable metadata to confirm that an organization is a legitimate and known credential issuer, CTDL complements this by offering a broader and deeper set of descriptive data about the issuer and its offerings. For example, CTDL can describe:

- The types of credentials the organization offers
- Accreditation or other third-party quality assurance relationships
- Geographic scope and jurisdiction
- Relevant competencies and skills
- Conditions for earning, renewing, or transferring a credential
- And many additional data points that provide a comprehensive view of the issuer and its role within the credentialing ecosystem

Each published CTDL record includes a Credential Transparency Identifier (CTID), a globally unique identifier that also functions as a persistent URI. A CTID is based on a standard UUID v4 format and looks like this: ce-e8a41a52-6ff6-48f0-9872-889c87b093b7

The URI structure based on CTIDs allows each record to be retrieved directly from the Credential Registry. For example:
https://credentialengineregistry.org/resources/ce-5ea303a9-0cba-42db-b828-38d2f1fb890d

CTIDs help verifiers and systems access reliable, descriptive data about an issuer or the credentials they offer.

More information about CTDL can be found on the Credential Engine Technical Site.

Governance Framework for Trust in Issuer Identity Registries

In W3C VC ecosystems, issuer identity registries can technically operate without formal governance structures.[3] However, to foster trust among stakeholders—issuers, verifiers, and credential holders—implementing a structured governance framework for issuer identity substantiation is essential. This project referenced Mayer, Davis, and Schoorman's Integrative Model of Organizational Trust[4], which emphasizes three core components: ability, integrity, and benevolence.

Ability: "Ability is that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain."[5] To effectively host and maintain issuer identity registries, an issuer identity registry host should possess technical competence in identity verification, security protocols, and data management.

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 actions are congruent with his or her words all affect the degree to which the party is judged to have integrity."[6] For issuer identity registries, integrity reflects how a relying party perceives a registry's adherence to established governance principles.

---

[3] Some text in this section sourced from 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 and Governance Framework for Issuer Identity Registries. Credential Engine and Digital Credentials Consortium. Published June 9th, 2025. Available here.

[4] 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

[5] Ibid.

[6] Ibid.

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."[7] In the context of verifiers, using an issuer identity registry refers to the degree to which the registry is perceived to act in the user's best interests.

The governance framework was developed through a collaborative and iterative process with members of the advisory group. It serves as both an example of the practices ecosystems need to establish trust and a template to help issuer identity registry implementers express their governance policies more efficiently and effectively.

The framework was created through a two-stage process:

- **Stage 1 – Input and Idea Data Collection**: Participants were introduced to the trust model and asked to contribute ideas about what makes a registry trustworthy. Contributions were mapped to the dimensions of ability, integrity, and benevolence to inform the framework's structure.

- **Stage 2 – Iterative Refinement and Synthesis**: Facilitators categorized and refined the collected data, focusing on identifying a minimum viable governance framework. A second live session was held to review a draft informed by Stage 1 input, allowing participants to offer clarifications and suggest additions. Based on this feedback, the framework was further refined—merging overlapping ideas, incorporating some new items, and finalizing the structure.

Governance Framework Development Results

The final output of this research was a governance framework designed to support trust in issuer identity registries through transparency, accountability, and clearly defined practices. The framework includes 48 guidelines organized into 7 thematic categories, each addressing specific aspects of trust:

1. **Registry Overview and Purpose:** Defines the scope, objectives, and operational principles of the issuer identity registry.

[7] Ibid.

2. **Governing Parties and Oversight:** Addresses the roles and responsibilities of the governing bodies and mechanisms for ensuring transparent, effective oversight of an issuer identity registry.

3. **Privacy Policy and Terms of Use:** Establishes the legal and contractual rights and obligations of the issuer identity registry with respect to data providers and data users.

4. **Issuer Information and Verification:** Details the processes and requirements for onboarding, verifying, and maintaining issuer data.

5. **Data Download Format:** Details the processes and policies regarding downloading issuer identity registry data.

6. **Technical Standards:** Establishes the technical foundation for an issuer identity registry based on specific standards used.

7. **Security and Operations:** Describes cybersecurity and technical operations information regarding how the issuer identity registry code is operated and maintained.

Each guideline within a category promotes one or more of the perceived trustworthiness factors: ability (A), benevolence (B), and integrity (I). For example, “Process for verifying issuer identity and legitimacy: Know Your Customer (KYC) process/other identification process” promotes both ability and integrity.

The framework is designed to be adaptable across different types of organizations that implement issuer identity registries, supporting a range of governance contexts and technical environments. This distribution underscores the framework's emphasis on integrity as a key factor in the perceived trustworthiness in issuer registries, while also highlighting the critical importance of ability and benevolence.

- **Integrity**: 40 of 48 guidelines
- **Ability**: 35 of 48 guidelines
- **Benevolence**: 29 of 48 guidelines

Organizations can utilize this framework to build trust in their issuer identity registry. By publicly documenting how each guideline is addressed, organizations can promote trust according to issuer, verifier, and credential holder expectations.

For full guidance and detailed criteria, refer to the full document: Governance Framework for Issuer Identity Registries. This resource provides the complete list of guidelines and definitions, and is designed to be adapted and reused by organizations developing their own governance policies. We encourage sharing and adapting the framework to meet the specific needs of issuer identity registry implementers.

Governance Implementation Approaches

DCC implemented a governance policy for its issuer identity registry as part of this project, applying the shared framework developed in collaboration with the advisory group. This policy formalizes oversight, roles, and responsibilities, and demonstrates how the governance guidelines can be put into practice to support trust and transparency. It also builds on DCC's existing open-source tools by adding a trust layer to its registry infrastructure.

While Credential Engine co-developed the shared governance framework, it has a responsibility to consult with its partners and stakeholders before applying it to its own registry. Beginning in the second half of 2025, Credential Engine will convene a working group to advise on governance requirements for integrating their issuer identity registry into the Credential Registry Publishing System. This system offers account management and workflows for assigning data publishing permissions. The working group's recommendations will ensure the governance model aligns effectively with existing publishing workflows and supports Credential Engine's transparency

Issuer Identity Registry Prototypes and Shared Features

To demonstrate how issuer identity registries can support trusted verification, both Credential Engine and DCC developed working prototypes using a shared set of technical specifications. These registries are designed to be queried by verifiers—such as employers, institutions, and credential evaluation services—who need to confirm that a digital credential was issued by a recognized and authorized organization. The prototypes implement selected open standards to

ensure consistent, secure, and interoperable access to issuer metadata across platforms and ecosystems.

Shared Features Across Prototypes

Both Credential Engine and DCC implemented issuer identity registry prototypes using a common technical foundation to promote interoperability, consistency, and trusted access to issuer information. These shared features ensure that verifiers can access and validate issuer metadata in a predictable and standards-aligned way, regardless of the hosting organization. However, this does not mean that both will have identical data.

- **Specifications Implemented**:
    - **OpenID Federation 1.0**: Limited to the relevant portions that define metadata and API endpoints for registry interoperability.
    - **DIDs**: Used as signed issuer identifiers for issuers, enabling cryptographic trust.
    - **CTIDs (optional)**: Used to link issuer entries to corresponding records in the Credential Registry described using the CTDL.

- **Endpoints Offered:**
    - **Trust Anchor Endpoint**: Provides metadata about the registry operator (i.e., Credential Engine or DCC).
    - **Issuer Endpoint**: Returns metadata about individual issuers based on their DID.
    - **Subordinate List Endpoint**: Lists all DIDs registered in the registry.

- **Common Metadata Properties**:
    - **Trust Anchor Endpoint**: Returns metadata about the registry operator including: DID, Legal Name, Logo URL, Homepage URL, Policy URL
    - **Issuer Endpoint**: Returns metadata about the issuer: DID, Organizational Name, Legal Name, Homepage URL, Logo URL or Logo in Base64, Optional: CTID, Credential Registry URI
    - **DID List**: List of registered DIDs.

Credential Engine Issuer Identity Registry Prototype

Before exploring the technical details, it is essential to distinguish the roles of the Credential Registry and the Issuer Identity Registry, which serve related but distinct functions within LER and verifiable credential ecosystems:

- **Credential Registry:** A CTDL linked open data infrastructure that publishes structured, machine-readable data about organizations, credentials, learning opportunities, skills, assessments, and related entities. Each top-level resource in the registry is assigned a globally unique Credential Transparency Identifier (CTID), which also forms part of its URI. The CTDL—built on W3C standards for linked open data—ensures that the information is interoperable, discoverable, and reusable across systems and applications. The Credential Registry does not issue credentials, serve as an issuer identity registry, nor store personally identifiable information.

- **Issuer Identity Registry**: A technical trust component that records structured, verifiable metadata about organizations authorized to issue credentials. It enables verifiers to confirm issuer identity by exposing signed metadata, including DIDs. While separate from the Credential Registry, it complements it by adding a layer of trust in the organizations behind the credentials.

Credential Engine developed a prototype issuer identity registry to demonstrate how trusted issuer metadata can be published and verified using open standards. This registry supports trust in verifiable credential ecosystems by allowing verifiers to confirm that credentials were issued by recognized, authorized organizations.

Although the prototype is not yet integrated with the Credential Registry Publishing System, it establishes the groundwork for a future in which issuers can publish both credential data and verified trust metadata through a single workflow. In the second half of 2025, Credential Engine will convene partners and stakeholders to shape the governance and workflow requirements for integration. This future state will enhance usability while maintaining transparency and accountability.

The planned architecture, illustrated in the figure 2 below, shows how credentialing organizations will set up accounts, publish credential and issuer metadata, and link that data to verifiable

credentials issued to individuals. Verifiers will be able to query minimal trusted issuer data from the issuer identity registry and optionally retrieve richer metadata from the Credential Registry.

Prototype Technology stack: The Web APIs for Maintaining Issuer Metadata and OpenId Federation APIs are written using .Net 8. For storage, it uses a PostgreSQL database. All the components of the prototype are deployed in an Azure Kubernetes Cluster with a container image built using a Redhat base image. There is a Swagger UI provided for ease of testing against the Web API.

Accessing the Prototype: The prototype is publicly accessible and can be tested via Swagger, providing a real-time demonstration of how issuer metadata is structured, signed, and retrieved: Credential Engine Test Issuer Registry Swagger UI

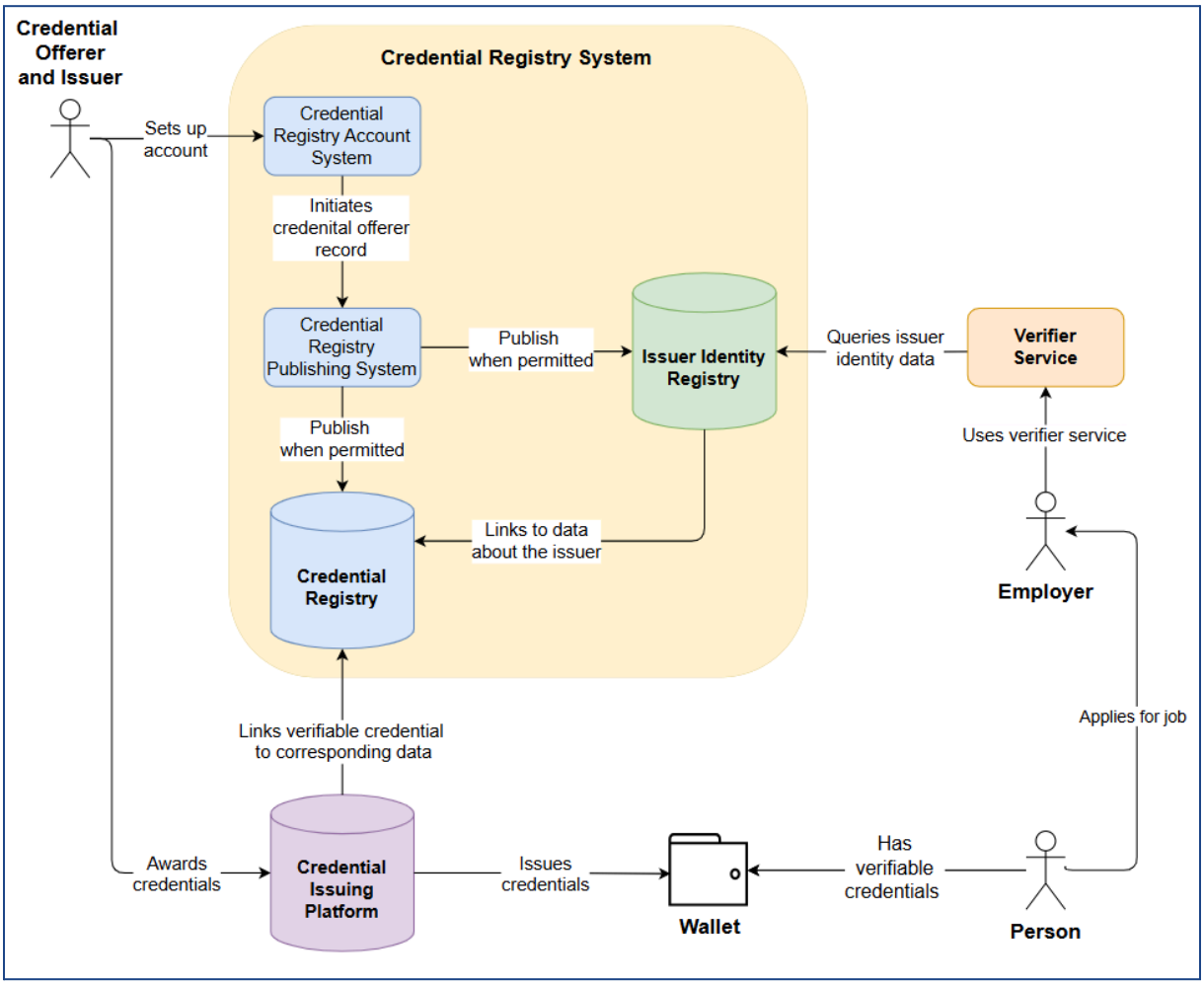
Prototype Features: The prototype utilized a design review process to confirm the requirements and test cases written prior to implementation. In addition to the shared specifications and design features described previously—including OpenID Federation 1.0, support for DIDs and CTIDs, and a common metadata schema—the Credential Engine prototype includes the following implementation elements:

- **API Endpoints for Maintaining Issuer Metadata**: Issuers submit metadata (including DID and CTID) to Credential Engine. These data are validated, signed, and made available to issuers via standard endpoints at /issuers/*. After the prototype phase, the Maintenance WebAPIs will be put behind an authentication and authorization layer so that only authorized issuers are permitted to make modifications.
- **API Endpoints for Verifiers**:
    - **Trust Anchor Information**
        - Retrieves metadata about Credential Engine as the registry host.
        - *Endpoint*: GET /oidfed/.well-known/openid-federation
    - **List of Issuer DIDs**
        - Returns a list of all issuer DIDs.
        - *Endpoint*: GET /oidfed/federation_list
    - **Issuer by DID**
        - Returns a signed JWT containing the issuer metadata.

    - *Endpoint*: GET /oidfed/federation_fetch?sub={did}

- **Security and Signature Verification**: All OpenId Federation metadata responses are signed using the EdDSA algorithm and formatted as JSON Web Tokens (JWTs). The registry validates signatures before returning a response. If verification fails, an error is returned to ensure authenticity and integrity.

Figure #2: Planned architecture for integrating issuer identity registry functionality into the Credential Registry Publishing System



DCC Issuer Identity Registry

The basic registry architecture was completed in two versions: a Node.js and SQLite system designed for local or server-based hosting, and a Node.js and DynamoDB system designed for AWS serverless hosting using AWS Lambda. The development followed a test-driven development (TDD) approach, where tests were designed first and server functionality was implemented afterwards.

In addition to the standard endpoints and base required system data, including the Federation Fetch Endpoint, Federation List Endpoint, and Federation Entity Configuration Request, the implementation also used the policy_uri to enable the trust anchor to indicate the location of the trust registry's governance.

A key element of registry governance is the requirement for participants to sign an entity statement before joining. This helps prove control of the DID. In the future, DID providers may be able to host their own Entity Statements (an OpenID Federation signed statement), reducing the need for the registry to manage them directly.

The implemented DCC prototype is hosted at two URLs: registry.dcconsortium.org and test.registry.dcconsortium.org. The registry's main functionality is to return metadata and DIDs for known and trusted issuers, with ongoing checks on known and trusted issuers to ensure compliance.

- **API Endpoints for Verifiers**:

  Host = [registry.dcconsortium.org, test.registry.dcconsortium.org]

  - **Trust Anchor Information**
    - Retrieves The DCC consortium metadata as the registry host.
    - *Endpoint*: GET [host]/.well-known/openid-federation

- **List of DIDs**
  - Lists all issuer DIDs in the registry.
  - *Endpoint*: GET [host]/subordinate_listing

- **Issuer by DID**
  - Returns a signed JWT of the issuer record.
  - *Endpoint*: GET [host]/fetch?sub={did}

Adapting DCC Applications for Issuer Identity Registry Use

The DCC developed and adapted several open-source libraries and applications to accommodate the prototypes created for this project. The project specifically provided an opportunity to streamline how DCC applications access registries and substantiate the identity of issuer DIDs.

Learner Credential Wallet (LCW) & VerifierPlus are open source applications that can read, verify, and share W3C VCs. LCW is a mobile application that verifies, stores, and shares VCs and OBv3. VerifierPlus is a standalone web application that can verify VCs and OBv3. Users of LCW can create a link on VerifierPlus that will share their credentials, enabling them to be verified in real-time.

Both LCW and VerifierPlus verify and display results for each credential indicating that credentials have been digitally signed properly, have not been tampered with since they were signed, have not been revoked, and have not expired. These applications also look up the issuer DID in registries that DCC has hosted prior to this project.

The DCC registries are JSON files hosted in Github repositories assigned for different categories of DCC entities including DCC member institutions, the broader community, and the sandbox. Entities are added to the registries via Pull Requests and approval by a DCC team member. Most often, entities are known prior to the Pull Request through participation in a DCC project or initiative. Each registry is an array of objects containing a DID, issuer name, website, and location for each issuer. The registries do not follow any standards and are likely only being used by the DCC.

As part of this project, the DCC adapted LCW, VerifierPlus and other libraries to use both the new prototype issuer identity registry and the legacy DCC registries. To do this, the DCC created a new repository called dcc-known-registries that contains the list of registries. This replaced the lists that were saved in the config files of the LCW and VeriferPlus. By doing this, it could be assured that both apps used the same registries, and that the list of registries would remain publicly available so that other issuer registries, like Credential Engine's, could be included in the list.

The DCC developed a new library, verifier-core, for integration into LCW and VeriferPlus to replace the code that previously performed verification. The DCC developed LCW and VerfiierPlus at separate times and leveraged slightly different approaches to verification and messaging. Using one library for both assured that applications would produce the same results for each credential in each application.

The issuer-registry-client is the library verifier-core used to access and retrieve issuer information from the registries. If the DID is found in one of the registries in the dcc-known-registries list, it will return the information about the issuer so that it can be displayed in the applications with a link to its governance document. If the DID is found in more than one registry, the applications will display the information found in each one. The DCC legacy registries will continue to be used. If the DID is not found in any of the registries, verifier-core returns an error message and the applications display a notification that the issuer cannot be found in a known registry.

Conclusion

Establishing trust within VC ecosystems is essential for enabling secure, efficient, and privacy-preserving digital interactions. This project has demonstrated the pivotal role of issuer identity registries in verifying the legitimacy of credential issuers and mitigating risks such as impersonation and fraud. By providing structured, verifiable metadata about issuers, these registries serve as a cornerstone of trustworthy digital infrastructure.

Based on the findings of this project, the following recommendations are offered to guide the development and implementation of issuer identity registries.

Key Recommendations

- **Adopt Open Standards and Specifications:** Use widely accepted standards like OpenID Federation 1.0 and DIDs, and CTDL to ensure systems are compatible, scalable, and interoperable across different platforms and regions. Verifiers should adopt tools and practices that align with these standards to complete the trust chain and ensure consistent verification.

- **Establish Clear Governance Frameworks:** Define who is responsible for managing the registry, how decisions are made, and what rules apply, helping to build transparency, trust, and accountability.

- **Ensure Interoperability and Scalability:** Design systems that can grow and seamlessly integrate with other registries and platforms, supporting a range of current and future use cases. This includes enabling verification tools to interact with registries across ecosystems.

- **Implement Robust Security Measures:** Protect data integrity by using cryptographic methods, such as digitally signing issuer data with JWKs, and validating those signatures before use.

- **Engage Stakeholders and Foster Collaboration:** Include a wide range of stakeholders including learners, issuers, verifiers, policymakers, and technical experts to ensure needs are addressed.

- **Provide Transparent Access and Documentation:** Ensure registry information and documentation is clear, accessible, and easy to use, enabling effective engagement and reliable use.

- **Plan for Continuous Improvement:** Build in regular reviews and updates to keep pace with changes in technology, policy, and user needs, ensuring long-term relevance and reliability.

Challenges and Considerations

As issuer identity registries continue to evolve and gain traction, their successful implementation depends on navigating several practical and technical challenges. These issues do not diminish the value or urgency of building trusted infrastructure—but they do require attention and collaboration from the outset. Key considerations include:

- **Specification Alignment:** Many specifications are broad in scope. For example, OpenID Federation 1.0 enables federated trust but does not natively support DIDs or CTIDs, which are essential for decentralized identity and linking credential data. Implementers must understand how to bridge gaps between specifications and data standards.

- **Adoption by Credential Issuers and Product Vendors:** Encouraging widespread adoption of open standards like W3C VC, Verifiable Credential Data Integrity, and OBv3 among credential issuers and product vendors is essential. These standards specify the use of DIDs and support CTIDs, promoting interoperability and trust across ecosystems.

- **Interoperability Across Diverse Systems:** Ensuring seamless interaction between various systems and registries requires ongoing collaboration and a shared commitment to evolving standards.

- **Stakeholder Engagement:** Sustaining participation from a broad range of stakeholders including learners, issuers, verifiers, policymakers, and technical experts is essential for the systems to meet real-world needs. However, coordinating this diverse input over time can be challenging without clear incentives, roles, and communication channels.

The challenges are surmountable through concerted efforts and collaboration. By advancing open standards, supporting inclusive and transparent governance, and committing to continuous improvement, we can build robust trust infrastructure. Such ecosystems will enhance the reliability of verifiable credentials and empower individuals across sectors to access and share trusted records of their achievements with confidence, speed, and security.

Future Research

This project identified several important areas for continued research and development to strengthen issuer identity registries and their role in trusted digital credential ecosystems. These

topics emerged through implementation work and discussions with advisory group participants. This list is not exhaustive. As verifiable credential ecosystems evolve, additional areas for investigation are expected.

- **Enhancing DID Support in OpenID Federation**: The current OpenID Federation 1.0 specification does not natively support Decentralized Identifiers (DIDs). Further research is needed to explore how DIDs can be more fully integrated.

- **Exploring Stakeholder-Specific Trust Requirements**: Governance was evaluated at a general level in this project, but trust expectations may vary between stakeholder groups (e.g., issuers, verifiers, credential holders). Future work could investigate how governance models can better address these differing perspectives.

- **Evaluating Implemented Governance Models**: The governance framework developed in this project was implemented by the DCC but has not yet been formally evaluated in practice. Future research could assess how well the model supports trust, usability, and long-term sustainability.

- **Clarifying Governance Practices for Key Rotation and Archival**: Managing key rotation and historical issuer data remains a challenge. The OpenID Federation specification does not currently promote retention of rotated keys, leading to gaps in continuity. Further work is needed to define how registries should handle these scenarios.

- **Expanding Applications for Learning and Employment Records (LERs):** Although this project focused on verifying issuer identity, issuer registries may also support broader LER-related use cases. Future research could explore how registries can link issuers to known credentials, accreditation status, or additional verified metadata.

Issuer identity registries are not theoretical constructs—they are practical trust infrastructure designed to solve real challenges in W3C Verifiable Credential ecosystems. This project established foundational models, specifications, and governance approaches that demonstrate what is achievable. While important challenges remain and further research is needed, the work to date provides a solid platform for continued progress. With sustained collaboration across sectors, issuer identity registries can scale to meet diverse needs and help ensure that verifiable credentials are trusted, usable, and empowering for all.

Acknowledgements

We extend our sincere gratitude to Walmart for their generous support, which made this initiative 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.

Appendix

Glossary of Terms

Badge

A visual, digital symbol of achieving a learning outcome or accomplishment; It often signifies the achievement of a skill, competency, qualification, certificate, membership, or service.

Credential

A set of claims made by an issuer. Examples of credentials include ID cards, licenses, diplomas, work eligibility claims, badges, and certifications. Credentials may be transmitted and processed as documentary evidence that a person has certain skills, status, or privileges.

Credential Transparency Description Language (CTDL)

An open schema developed and maintained by Credential Engine for describing information about credentials, learning opportunities, skills, organizations, and related data. Built on W3C standards for linked open data, CTDL enables consistent, machine-readable representations that support transparency, discoverability, comparability, and interoperability across education and workforce systems.

Cryptography

Cryptography is the practice of protecting information through the use of coded algorithms, hashes, and signatures. Digital credentials that are cryptographically signed are tamper-evident, machine-verifiable, and persistently accessible to learners, without dependence on the issuing organization to store or manage ongoing access to the data.

Decentralized Identifier (DID)

A cryptographically verifiable identifier embedded in a credential. DIDs are verifiable, persistent, and do not require a centralized registry or database.

Digital Credential Wallet

A digital credential wallet is an application that allows users to store, manage, and share credentials. Some wallets are generic like Apple wallets and others are specialized to support W3C VCs.

Holder

The person or entity about whom the claim in the credential is made. For example, a college graduate who has been issued a Bachelor's Degree.

Interoperability

The ability of different devices, software, or systems to successfully talk to each other. Interoperability is a characteristic of a product or system to work with other products or systems.

Issuer

1. An organization or person who makes a claim about a person. For example, a university issuing a degree to a graduate.
2. A software or system that generates and signs a credential.

Issuer Identity Registry

A machine-readable digital service that publishes structured data about organizations that issue VCs. These registries do not issue credentials or verify their contents. Instead, they serve as a trust layer for verifying issuer identity, helping verifiers determine whether an issuer is known, governed, and trusted within one or more ecosystems.

Key Rotation

Key rotation refers to the process of changing a public/private key pair which belongs to an entity. This means that a new public key will need to be provided to relevant entities and that previously signed credentials or statements may become invalid. Key rotation can occur for various reasons, including private key compromise, policy requirements, or lost private keys.

Learning and Employment Record (LER)

A document of any achievement related to learning or work. It may be used to qualify the learner or worker for hiring or advancement. Employment records, academic transcripts, professional licenses, micro-credentials, badges, and degrees are all examples of LERs.

LERs issued as Verifiable Credentials (LERs issued as VCs)

LERs issued using W3C Verifiable Credentials, Open Badges 3.0, and Comprehensive Learner Record 2.0 standards.

Micro-credential

A credential that addresses a subset of field-specific knowledge, skills, or competencies; often developmental with relationships to other micro-credentials and credentials.

Open Badges 3.0
An open standard put forth by 1EdTech for issuing learning and training credentials as Verifiable Credentials.

OpenID Federation 1.0 Specification
A specification for describing how two entities that would like to interact can establish trust between them by means of a trusted third party.

W3C Verifiable Credential (W3C VC)
A credential issued in alignment with the World Wide Web Consortium (W3C) Verifiable Credentials specification. W3C VCs are a set of claims and metadata with an attached cryptographic proof.

Verifier
An entity or software that performs verification of credentials by confirming the authenticity, status, applicability, and/or conformance of a credential to expectations or requirements.

List of Registries and Specifications Evaluated

Note: this list was inspired by and partially sourced from the IIW 38 session Day 2 / Session 7 / Space I session "Trust Registry FACE OFF!!" with Andor K, Mathieu Glaude, and Sam Curren.

1. ACDC (IETF)
2. ASU The Trusted Learner Network Ecosystem
3. Bhutan implementation
4. Blockcerts Public Key Registry
5. Country-specific master list (Germany)
6. DIF Credential Trust Establishment
7. PKI (Public Key Infrastructure)
8. EBSI Trust Chains
9. ETSI Trust List
10. EU COVID certificates
11. EU Digital Identity and Trust ecosystem Digital Wallet (eIDAS)

12. EU EIDAS scheme
13. European Digital Credential for Learning (EDC)
14. Fraunhofer TRAIN (eSSIF-Lab TRAIN)
15. GAIN
16. Gaia-X Federation Services Trust Management Infrastructure IDM.TRAIN
17. GLIEF
18. Global acceptance network trust registry (GAN)
19. ICAO COVID certificates
20. ICAO master list
21. ICAO public key directory
22. ISO mDL ISO/IEC 18013-5 standard
23. ISO mDL ISO/IEC 18013-5, AAMVA VICAL implementation
24. Incommon
25. Issuer Resolution (defunct)
26. NIST Authenticator Assurance Levels
27. Northern Block Orbit Trust Registry
28. OpenID Federation
29. P1484.2 LER - IEEE
30. PTCF-CCP
31. Regi-Trust
32. SAML
33. State of CA OpenCred
34. TNO-SSI-LAB Credential Catalog
35. Taiwan implementation
36. Trust over IP Trust Registry Protocol v2
37. UBICUA SSIDDI
38. Velocity Network
39. W3C CCG Verifiable Issuers and Verifiers 0.1

Specification Information and Evaluation Template

Specification Information and Evaluation Template	
Name	Name of trust registry implementation or specification
Description	Quoted description of the implementation or standard from the implementation/standard website
Type	• Weakly specific standard - Standard suitable for many use cases, potentially including LERs or other areas • Highly specific standard - Standard for a specific use case, potentially unrelated to LERs • Combination of standards - A mix of standards unified into a larger group • Implementation - A custom implementation which does not follow any particular existing standard
Trust anchor name	What the trust anchor is called in the specification/implementation
Link to registry	A link to a live version of the registry implementation
Format	• API-based • Data file-based • Unclear
Open/closed publication	Open-source Closed-source
Standards used	Which other standards are used in this standard/implementation (e.g. JSON-LD, DIDs, NIST standards, X.509, ETSI TS 119 612)
Stores registry history	Does the implementation store previous versions of the registry which can be accessed by the public?
Usability	Any notes provided by the spec/implementation on the usability of the system
Heartbeat	How does the registry signal to users that it is still being updated?
Signed	Is the registry output cryptographically signed?
Revocation	How does the registry signal that an issuer is revoked?
Different trust anchors....	How do different trust anchors interconnect? Are they collaborative? Competitive? Do they point to each other?
Governance	How (if mentioned) does the specification support the governance of the registry?
Draft/Provisional status	Status of the implementation/registry
Informational URLs	Reference information

Advisory Group Documentation and Resources

To support transparency, collaboration, and broad participation, all advisory group meeting materials were documented, organized, and archived in a publicly accessible folder. Each meeting includes a recording, slide deck, and reference materials to support asynchronous engagement. These materials are available for anyone to view.

Charter: Issuer Identity Registry Advisory Group Plan and Charter (ACCEPTED)_Version 2_October 2, 2024

Meeting Folders

- Meeting 1 2024-Sept-4: Issuer Registry Advisory Group Kickoff Meeting
- Meeting 2 2024-October-2: Issuer Registry Advisory Group
- Meeting 3 2024-November-13: Issuer Registry Advisory Group
- Meeting 4 2024-December-4: Issuer Registry Advisory Group
- Meeting 5 2025-January 8: Issuer Registry Advisory Group
- Meeting 6 2025-February-5: Issuer Registry Advisory Group
- Meeting 7 2025-March-12: Issuer Registry Advisory Group
- Meeting 8 2025-April-2: Issuer Registry Advisory Group
- Meeting 9 2025-May-28: Issuer Registry Advisory Group

Technical Subgroup: In addition to the scheduled meetings, a technical subgroup convened to focus on implementation issues. Its session is also archived:

- Issuer Registry Technical Subgroup Meeting 2025-March-19

Educational Outreach and Community Engagement

In an effort to promote the understanding of issuer registries as vital components of trust in W3C VC ecosystems, Credential Engine and the DCC put forth a number of educational materials. Critical to the adoption and effective use of issuer registries is the understanding across stakeholder groups of how they function, the advantages they offer, and how they can be integrated in existing credentialing systems. The project team disseminated information on issuer registries in a number ways including:

- **Blog Posts:** We published Informative articles to explain key concepts around issuer registries and their role in digital credentialing.
    - Issuer Registries — Layering Trust for Verifiable Credential Ecosystems
    - Selecting the OpenID Federation specification for the DCC and Credential Engine Issuer Registry Project
    - Issuer Registries: Establishing trust, privacy, and efficiency in verifying credential issuers
- **Conference Sessions:** The project team gave presentations and facilitated discussions to share insights and gather feedback on issuer identity registry implementations from both technical and non-technical audiences.
    - OID25: Developing A Governance Framework for Learning and Employment Record (LER) Issuer Registries
- **Webinar:** DCC and Credential Engine presented at the Groningen Declaration Network Conversation Series: Understanding Credential and Skill Transparency and Interoperability.

These efforts were designed to build a shared understanding among diverse stakeholders, including educational institutions, employers, policymakers, and technology providers, about the importance of issuer registries in establishing trust within verifiable credential ecosystems.