



Issuer Registries

Establishing trust, privacy, and efficiency in verifying credential issuers

What is an issuer registry?

An issuer registry is a secure, trustworthy digital list containing verifiable information about organizations that issue credentials. These credentials can include a range of documents from state issued IDs or driver's licenses, vaccination cards, to achievements like degrees and certificates. These issuers, which could include associations, education and training institutions, and government agencies, usually must meet defined criteria before they are admitted onto a registry. An issuer registry ensures that anyone can near-instantly and easily verify that an organization listed as a credential issuer is authentic and authorized to issue the specified credentials.

For credentials issued as [W3C Verifiable Credentials and Open Badges 3.0](#) – two widely referenced open standards for education and training credentials – issuer registries can significantly enhance system trust by providing a reliable framework for these tamper-proof credentials. Issuer registries act as intermediaries of trust by enabling verifiers to confirm issuer identities without revealing the act of the verification process to the issuer. This approach ensures that credential holders maintain privacy when sharing their credentials.

Why do we need issuer registries?

Issuer registries offer numerous advantages by providing a secure and verifiable way to confirm the legitimacy of credential issuers. Compared to traditional methods of listing issuers as hard copy, paper records or web pages, they enhance trust, streamline verification processes, and reduce fraud, and benefit a wide range of organizations including:

- **Universities proving that they are authorized to issue degrees:** An issuer registry can identify the issuer of a degree or diploma as legitimate according to the standards of a governing body such as an accrediting body. This enables degrees to be instantly recognized and trusted across different consumers, including institutions and employers.
- **Training providers or institutions that issue professional certifications, continuing education units, or licenses:** For example, medical professionals must be licensed by trusted identifiable issuers.
- **States issuing digital driver's licenses or IDs:** An issuer registry can ensure that state agencies, like DMVs, are the actual issuers of a driver's license. They use common standards and specifications to promote consistency across jurisdictions.
- **Employers looking for trustworthy verification that a candidate has specific credentials necessary for a role:** Anyone, including the credential holder or an employer, can search to confirm whether or not an issuing organization is listed on an issuer registry.

Example use case

Consider a technical institution issuing welding certifications. Issuer registries addresses the following possibilities:

- **Impersonation or fraud:** A bad actor could claim to be the organization and issue fake credentials. The institution's existence on an issuer registry means that its identity has been recognized by a legitimate governing body. In this case, the governing body could be a state workforce board.
- **Illegitimacy:** The organization may claim to be authorized to issue a license for welding engineers but fails to meet the criteria set by a governing body, such as using a standardized assessment process. In this case, the governing body would only recognize the institution on the issuer registry if they met the criteria.
- **Inefficiency:** In scenarios like job offers, where time is of the essence, issuer registries enable near-instantaneous validation, avoiding manual checks.

If the technical institution is listed on an issuer registry, an employer vetting a job candidate with a credential from this institution can quickly verify its identity and confirm that it is qualified to issue welding engineer credentials. This exchange protects all involved parties—the credential holder, the institution, and the employer.

Application of issuer registries

The process of verifying credentials across locations, institutions, and jurisdictions can be time-consuming, often taking days or even weeks. For example, as of 2024, in the U.S. state of Maryland, an applicant for a nursing license who was trained in another state waits 4 to 6 weeks to have their education approved as “substantially equivalent” to the training offered in the state.¹ Licensed Marylanders seeking employment in other states must also request verification and pay a fee in person or through the mail. An issuer registry could reduce the time spent on reviewing credentials, especially when they are issued as Verifiable Credentials (VCs). The VC data model enables the embedded rich metadata describing the applicants skills to be cryptographically verified instantly. This process can include confirming the issuer's identity by validating that it is listed on a trusted, governed issuer registry.

The prevalence of fake credentials, including degrees, undermines trust in legitimate ones. In a 2023 Canadian survey of university registrars, 54.7% reported that they do not “feel confident detecting fake degrees.”² Issuer registries can be paired with cryptographically supported standards such as [Verifiable Credentials](#) (VCs), providing a trustworthy way to verify the origin, authenticity, and meaning of credentials. There are multiple layers of trust provided for VCs issued by institutions on an issuer registry, so that fraudulent credentials are identified early on and the reputation of legitimate credentials and institutions are preserved.

In our increasingly digitized world, users often need to submit personal information to access services. Issuer registries can enforce rules to protect user privacy. For instance, digital drivers licenses that are issued under a specific issuer registry can be required to provide each data field separately (name, birth date, ID, height, weight, home address, vehicle qualifications), thereby withholding irrelevant information such as one's home address when verifying.³ Additional trust comes with the verifier's ability to determine that the provided information was put forth by an institution on an issuer registry.

¹ Maryland Department of Health. (2024, August). *Frequently Asked Questions (FAQs) About RN/LPN Licensure and APRN Certification*. <https://mbon.maryland.gov/Documents/FAQs-Licensure.pdf>

² Carmichael, J. (2023, June). *Understanding Fake Degrees and Credential Fraud in Higher Ed*. <https://evollution.com/programming/credentials/understanding-fake-degrees-and-credential-fraud-in-higher-ed>

³ Riley, T. & Williams, Z. (2024, February). *Mobile Driver's Licenses Face Privacy Scrutiny Ahead of NY Pilot*. <https://news.bloomberglaw.com/tech-and-telecom-law/mobile-drivers-licenses-face-privacy-scrutiny-ahead-of-ny-pilot>

Additional considerations

The function of an issuer registry within a credential ecosystem, whether pertaining to Learning and Employment Records (LERs) or IDs, can be influenced by the role of verifiers. A “verifier registry,” like an issuer registry, is a digital list of entities, ensuring that only authorized entities conduct verification. Verifier registries are particularly useful when sharing or validating sensitive personal information, like financial records, healthcare information, or identity as it relates to government benefits and services. A verifier registry can help a credential holder have trust in the process of sharing their credentials, knowing that they are only sharing with authorized parties.

Trust, privacy, and efficiency are all complex but important components of digital credentialing ecosystems. Issuer registries play a key role in supporting these and other benefits.

More information

The Digital Credentials Consortium (DCC) and Credential Engine are working together to research and explore the governance and technology needs for implementing issuer registries within Learning and Employment Record (LER) ecosystems. To get involved, we invite you to:

- Join the Issuer Registry Advisory Group: Participate in discussions and deliverables to build shared understanding and contribute to project success. You can learn more about this opportunity [here](#) and sign up [here](#).
- Participate in the pilot: Participants will engage in testing a functional issuer registry and provide feedback and insights to refine the model for broader implementation. Invitations will be sent out later.
- Stay informed: We will continue to provide updates on this project! Subscribe to [Credential Engine’s newsletter](#) and [DCC’s newsletter](#) to stay current.
- Learn more: Read more about this work and partnership [here](#) and [here](#).

Contact us at info@credentialengine.org or digitalcredential@mit.edu to learn more about this project.

September 25, 2024

This work is licensed under the [Creative Commons Attribution 4.0](#) International License. We encourage reuse and remix of this resource with attribution to Credential Engine and Digital Credentials Consortium.

