DIGITAL CREDENTIALS IN EDUCATION: FROM STANDARDS TO AN INTEROPERABLE HIGHER EDUCATION ARCHITECTURE

Andrei-George BUHNICI[1], Ciprian DOBRE[2]

Abstract. *Digital credential standards address different parts of the credential lifecycle and they do not need to be treated as substitutes of one another in every case. This paper compares W3C Verifiable Credentials, Open Badges 3.0, European Digital Credentials for Learning, Credential Transparency Description Language, and provider-controlled solutions, and proposes an interoperable architecture for managing digital credentials in higher education. The idea behind the proposed solution is to store a common internal object that depicts a credential, while adapters provide bidirectional import and export operations for Open Badges and EDC. Europass supplies the required services for signing EDCs, and the CTDL links add public information about programmes, providers and competencies. By separating institutional data from exchange formats and trust mechanisms portability is enhanced.*

Keywords: Digital credentials, Verifiable Credentials, Open Badges, European Digital Credentials, Credential Transparency Description Language

DOI 10.56082/annalsarsciinfo.2026.2.44

1. Introduction

Higher education increasingly uses digital credentials for degrees, course completions, micro-credentials and other competencies of students [1]. A credential must identify the issuer and learner, describe the award, support verification and remain usable outside the system that created it. These requirements are often discussed together, although in the current landscape they are provided by different standards and services.

W3C Verifiable Credentials (VC) [2] defines a general model for verifiable claims. Open Badges 3.0 [3] applies that model to educational achievements. European Digital Credentials for Learning (EDC) [4] represents learning records through the European Learning Model (ELM) [5] and integrates with the Europass [6] services. CTDL [7] links credentials to structured information about providers, competencies

[1]Eng., Faculty of Automatic Control and Computers, University "Politehnica" of Bucharest, Bucharest, Romania, (andrei.buhnici@stud.acs.upb.ro).
[2]Prof., Faculty of Automatic Control and Computers, University "Politehnica" of Bucharest, Bucharest, Romania, (ciprian.dobre@upb.ro).

and pathways, but not learner specific awards. These approaches therefore solve related, but different, parts of the same problem.

This paper examines how higher education can use these approaches together instead of selecting one as a universal format. It first assigns a clear role to each approach, then identifies the data, governance and infrastructure requirements that affect interoperability. Based on this analysis, the paper proposes a solution that uses a common internal credential object with adapters for importing and exporting Open Badges and EDC records, integrates with Europass services for EDC, and links CTDL to learner specific credentials for public contextual information.

2. Related Work

Previous work covers both technical standards and the institutional use of digital credentials. Specifications from W3C, 1EdTech, the European Commission and Credential Engine define the available data models and services. However, adoption research shows that issuing a technically valid credential does not ensure that institutions or employers will recognize it by default [8]. The RSA Digital Badging Commission also identifies trust, verification and recognition of digital credentials as challenges that have not been resolved [9].

Implementation studies add a more practical perspective of system integrations. A cross-border EBSI pilot reported difficulties involving ecosystem governance, transcript schemas, wallets and digital identity integration [10]. Therefore, existing work explains individual standards or deployment barriers but does not define a higher education data model that can preserve one credential record while producing Open Badges and EDC representations and linking it with CTDL context. This integration problem is the focus of this paper.

3. Methodology

The review uses available specifications and implementation documentation for W3C VC, Open Badges 3.0, EDC and CTDL, together with policy and implementation evidence. For each approach, the analysis identifies what each represents, how credentials are issued and verified, how lifecycle changes are handled, what can be exchanged outside the source system and what dependencies on external services or governance policies are required.

Because the approaches operate at different technical and organizational levels, they are compared by their respective function rather than being analyzed as equivalent alternatives. An aspect outside an approach's intended role is not treated as a deficiency. For example, CTDL describes credentials and related entities but does not issue awards to individual learners. Provider-controlled solutions are considered as an operational category because their capabilities depend on the

formats and services implemented by each product. The criteria used to evaluate digital credential formats are summarized in Table 1.

Table 1. Analytical Framework Used in the Review

Evaluation criteria	*Question applied in the analysis*
Role and data represented	Does the approach represent a learner award, descriptive information, a trust layer or an operational service?
Issuance and lifecycle	How are creation, proof, expiration and revocation supported where applicable?
Exchange and verification	Can credentials be imported, exported and verified outside the system that created them?
Governance and infrastructure	What standards, trust services, registries or platforms does the approach depend on?
Educational use	Which achievement types are best supported, and which complementary components are required?

4. Results

The results assign a distinct role to each approach, identify the missing integration between those roles and use the resulting requirements to define the proposed architecture.

4.1. Roles of the Selected Approaches

4.1.1. W3C Verifiable Credentials Data Model

The W3C VC Data Model [2] provides a flexible framework for representing verifiable claims issued to holders and presented to verifiers. Cryptographic proof mechanisms can establish authenticity and integrity, and optional status mechanisms can support suspension or revocation. VC does not define how learning outcomes, assessments, credits or qualifications must be represented. Therefore, VC is mostly a general trust and exchange framework.

4.1.2. Open Badges

Open Badges 3.0 [3] is an education-oriented standard for portable achievements such as skills, course completions and micro-credentials. An awarded badge is represented as a VC compatible credential and includes structured fields for the achievement, award criteria, evidence and alignment with external frameworks.

The format provides more structured educational detail than the generic VC, but external use still depends on clear criteria and consistent metadata between institutions.

4.1.3. European Digital Credentials for Learning

European Digital Credentials for Learning [4] are multilingual, electronically sealed learning records based on ELM [5]. They can represent diplomas, certificates and micro-credentials and can use the Europass infrastructure for creation, issuance, storage, sharing and verification [6]. Their electronic seals operate within the eIDAS trust framework [11]. EDC therefore combines a detailed European education model with shared services. The downside is that institutions must map their data to ELM and meet the relevant seal requirements.

4.1.4. Credential Transparency Description Language

CTDL [7] is a linked data schema for publishing information about credential offerings, providers, competencies, assessments, pathways and related learning opportunities. It does not assert that a specific learner earned an award and does not replace the proof or status of an issued credential. In the proposed architecture, CTDL supplies stable public context that can be linked from either an Open Badges or an EDC representation.

4.1.5. Proprietary Credential Solutions

Provider-controlled credential solutions are operational products rather than formats. They usually combine design, issuance, storage, sharing and hosted verification within a unified platform. Portability depends on the product's import, export and independent verification capabilities. The comparison therefore treats them as a deployment category and not as another credential standard.

4.1.6. Functional Comparison

Table 2 describes each approach according to the function it can perform in an interoperable higher education context. The comparison shows that the approaches should be connected through explicit mappings rather than forced into a single technical role.

Table 2. Formats comparison of roles and characteristics

Approach	*Primary role*	*Import or export use*	*Dependencies and Limitations*
W3C VC	Generic claim and proof model	Framework for compatible credential formats	Generic schema for achievements leads to difficulties regarding portability
Open Badges 3.0	Learner achievements or micro-credentials	Bidirectional badge exchange as a VC compatible credential	Institutional criteria and competency alignments required between higher education institutions
EDC	European learning record	Bidirectional EDC exchange through Europass	Depends on ELM mapping and an eIDAS compliant seal approved by the European Commission
CTDL	Public description of offerings, providers, competencies and pathways	Publication and linking of contextual data	Requires a separate learner specific credential
Provider-controlled solution	Operational issuance and management product	Depends on product import and export support	Requires a separate solution for independent import, export and verification for portability

The comparison does not identify a universal complete replacement for the others. W3C VC supplies a generic proof model, Open Badges and EDC represent learner awards for different ecosystems and CTDL describes the public context around those awards. A higher education institution therefore needs an internal representation that is independent of any exchange format.

The central interoperability problem is data mapping. The same institutional award may need an Open Badges representation for broader badge ecosystems and an EDC representation for Europass compatibility regarding portability within the European context. Shared fields, such as issuer, learner, achievement, outcomes, criteria, evidence, dates and status, can be stored once, while format adapters translate them into the required external structures. Format specific properties must be retained so that import and export do not discard information.

Successful exchange also requires consistent descriptions. Two systems may validate the same credential but still interpret it differently when learning outcomes, award criteria or qualification levels are incomplete. Institutional rules for these fields and links to recognised frameworks are therefore part of interoperability, not optional documentation [8], [9].

Independently developed solutions can support this model if they implement the read and write operation for the selected standards and allow credentials to be verified without the original hosted service.

4.2. Requirements for Institutional Interoperability

The previous analysis identifies three requirements that the architecture must address: consistent academic data, clear institutional governance and integration with external trust and service infrastructure.

First, the common record must use consistent rules for learning outcomes, award criteria, evidence and competency alignments. Open Badges and EDC provide fields for this information, but institutions decide how the fields are completed. Without a shared method, credentials remain difficult to interpret outside their original context [8], [9].

Second, the higher education institution must define who should issue credentials, how quality is assured, how status changes are authorised and how micro-credentials relate to formal qualifications. The European Union Council recommendation on micro-credentials treats these governance and recognition questions as requirements that accompany technical implementation [12].

Third, the architecture must support the infrastructures through which each credential format is issued, exchanged and verified. Evidence from the EBSI pilot shows that institutional onboarding, wallet support, compatible data models and identity integration present implementation challenges beyond signature validation [9]. These requirements should be treated through separate adapters, ensuring that institutional records stay independent of external platforms and services.

4.3. The Proposed Interoperable Higher Education Architecture

Fig. 1 presents a conceptual architecture derived from the roles of the formats discussed in Table 2 and the requirements identified in Section 4.2. Its central design choice is a common credential object stored in the higher education institution database. Open Badges, EDC and CTDL are connected to this object through separate adapters, so they remain distinct external representations rather than competing sources of truth.

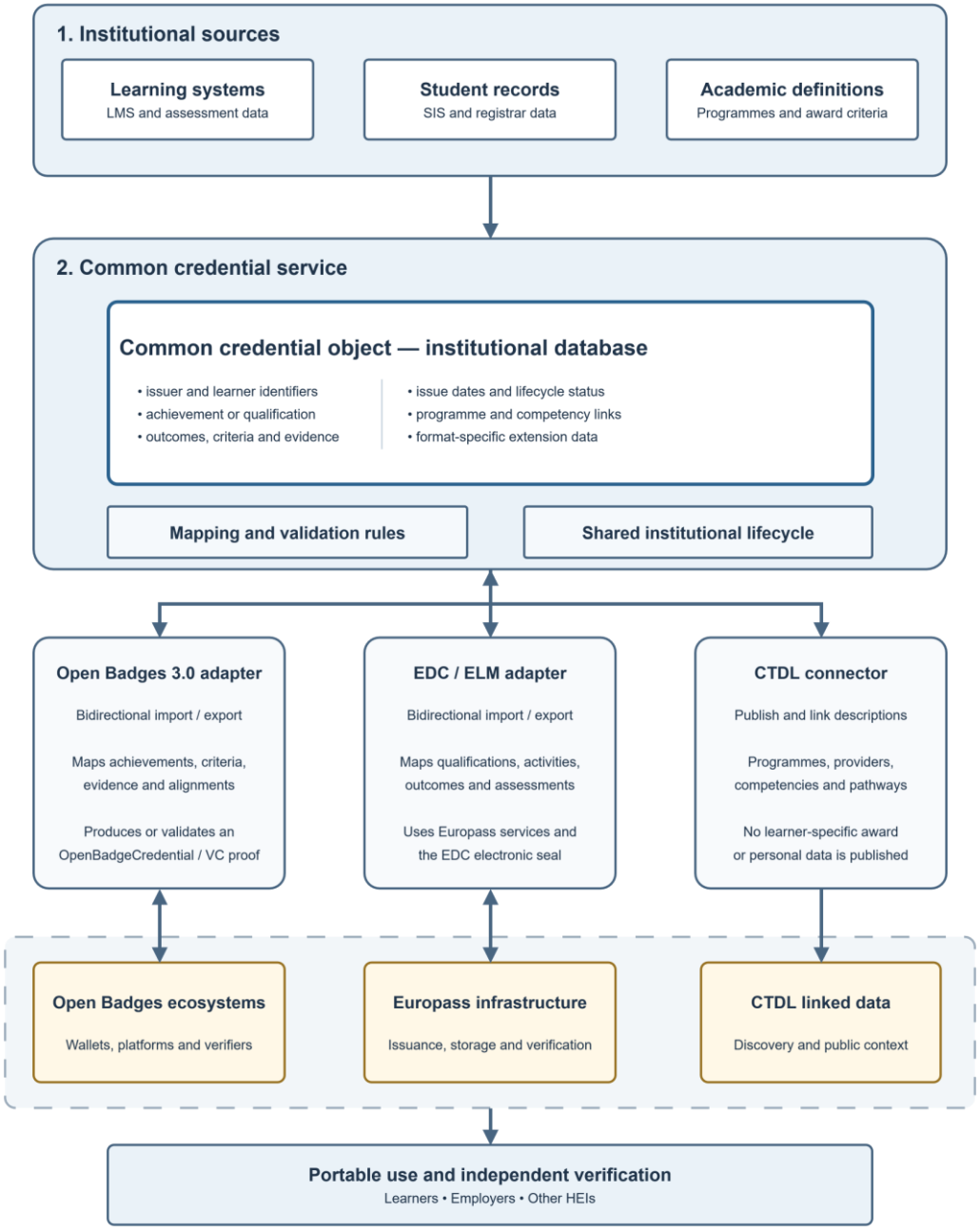

Fig. 1. Interoperable higher education architecture based on a common credential object and format specific connectors.

The higher education institution's learning management, student information and registrar systems supply data to a common credential service. For each award, the service stores a common object containing issuer and learner identifiers, the achievement or qualification, learning outcomes, criteria, evidence, timestamps, lifecycle status and links to programmes or competencies. This object is the institutional source of truth. External credential files are generated from this common record in the required format.

The Open Badges adapter maps the common object to and from a VC based credential for achievements and micro-credentials. The EDC adapter maps the same core data to and from ELM and uses Europass services for EDC issuance, storage, sharing and verification. Because the formats do not have identical fields, each imported record retains its original file and any format specific extension data, allowing mappings to be revised without losing source information.

The CTDL connector has a different role. It publishes or links non-personal descriptions of programmes, providers, competencies and pathways. The common object stores the relevant CTDL identifiers, allowing both an Open Badges credential and an EDC record to point to the same public context without treating CTDL as a learner credential.

Trust and lifecycle processing remain format specific at the system boundary. Open Badges credentials are validated using their VC compatible proof and status information, while EDC records are checked through their electronic seal and Europass verification process. Internally, the higher education institution maintains one lifecycle state for the award and translates changes into the status mechanism supported by each exported representation.

On export, the service generates the format selected for the destination ecosystem. On import, it validates the native credential, maps supported fields into the common object and preserves the original data together with the proof. Learners can therefore receive portable Open Badges or EDC records, while employers and partner higher education institution can verify each record through its native mechanism and follow CTDL links for additional programme or competency information.

The architecture does not assume that Open Badges and EDC are semantically identical. Its purpose is to preserve their shared data, expose differences through explicit mappings and prevent separate institutional databases for each format. Issuer authorisation, quality assurance, recognition policy and participation in external governance frameworks remain institutional decisions.

5. Limitations and Future Research

The comparison is based on specifications, official documentation and a limited set of implementation studies rather than measurements from deployed higher education systems. It does not evaluate cost, usability, performance or adoption rates, and findings about provider-controlled products remain general because products differ. The proposed architecture is conceptual and has not yet been implemented or tested with real issuers, learners or verifiers.

Future work should implement the common credential object and both adapters in a higher education pilot. The evaluation should measure round-trip preservation of required fields, validation success after import and export, consistency of lifecycle updates and the amount of format specific data that cannot be mapped. Testing should also assess issuer governance, recognition procedures and the usability of Europass and workflows based on badges.

6. Conclusions

The analyzed approaches have distinct roles that might overlap on certain features. W3C VC supplies a generic verifiable claim model. Open Badges represents portable achievements. EDC represents European learning records and uses Europass services. CTDL publishes programme, provider, competency and pathway information.

Higher education should not store each output format as a separate source of truth. A common credential object can hold shared award data, while Open Badges and EDC adapters provide bidirectional import and export and CTDL links add public context.

The architecture can be evaluated through concrete tests: required fields should survive round trip conversion, imported records should retain their original proofs, exported records should pass native verification and lifecycle changes should remain consistent across representations. Issuer authorization, quality assurance and recognition remain institutional responsibilities and must be evaluated in a pilot.

REFERENCES

[1] UNESCO, *Digital Credentialing: Implications for the Recognition of Learning across Borders* (UNESCO, Paris, France, 2021).

[2] *Verifiable Credentials Data Model v2.0,* [https://www.w3.org/TR/vc-data-model-2.0/].

[3] *Open Badges 3.0 Implementation Guide,* [https://standards.1edtech.org/open-badges/guides/standards/v3p0/impl].

[4] *European Digital Credentials for Learning,* [https://europass.europa.eu/en/european-digital-credentials].

[5] *European Learning Model: Data Model Browser,* [https://europa.eu/europass/elm-browser/index.html].

[6] European Parliament and Council of the European Union, *Decision (EU) 2018/646 on a Common Framework for the Provision of Better Services for Skills and Qualifications (Europass)*, Off. J. Eur. Union L 112, 42–50 (2018).

[7] *Credential Transparency Description Language (CTDL),* [https://credentialengine.org/credential-transparency/ctdl/].

[8] D. Gibson, N. Ostashewski, K. Flintoff, S. Grant and E. Knight, Educ. Inf. Technol. 20, 403–410 (2015).

[9] RSA Digital Badging Commission, *From Skills to Growth: A Plan for Digital Badging in the UK* (Royal Society of Arts, London, United Kingdom, 2025), [https://www.thersa.org/reports/digital-badging-commission/].

[10] E. Tan, E. Lerouge, J. Du Caju and D. Du Seuil, Big Data Cogn. Comput. 7, 79 (2023).

[11] European Parliament and Council of the European Union, *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, Off. J. Eur. Union L 257, 73–114 (2014).

[12] Council of the European Union, *Council Recommendation of 16 June 2022 on a European Approach to Micro-credentials for Lifelong Learning and Employability*, Off. J. Eur. Union C 243, 10–25 (2022).