



Publisher

<http://jssidoi.org/esc/home>

RECOGNISING EMPLOYEES' COMPETENCES THROUGH VERIFIABLE MICRO-CREDENTIALS: ALIGNING HIGHER EDUCATION AND EMPLOYERS' NEEDS IN THE DIGITAL ERA*

Daiva Stanelytė

Klaipėdos valstybinė kolegija / Higher Education Institution, Jaunystės g. 1, LT-91274 Klaipėda, Lithuania

E-mail: d.stanelyte@kvk.lt

Received 15 October 2025; accepted 30 December 2025; published 30 March 2026

Abstract. Labour markets in the digital and Industry 5.0 era increasingly expect timely and trustworthy evidence of what employees can actually do, not only which formal qualifications they hold. However, employers often face information asymmetries: CVs and traditional diplomas provide limited insight into specific competences, especially when they are developed through short courses and non-formal learning. This paper examines how verifiable micro-credentials and digital badges can reduce these asymmetries by making learning outcomes, assessment and evidence transparent and machine-readable for employers. Based on a narrative, concept-centred review of 30 peer-reviewed articles (2016–2025), the study develops a three-layer model (pedagogical–assessment, technological–verification, recognition–policy) and a minimum interoperability profile for micro-credentials. The model links competence needs signalled by employers to learning outcomes, assessment tasks and authentic artefacts that can be recognised both in formal higher education and in flexible, work-based and non-formal settings. The paper outlines practical decision rules and an implementation roadmap for higher education institutions to issue verifiable micro-credentials that are readable and useful for employers. The contribution is an actionable framework that supports skills-based recruitment, internal mobility and upskilling strategies while keeping the recognition of employees' competences at the centre.

Keywords: verifiable micro-credentials; digital badges; employee competences; skills recognition; labour market signalling; employers' needs; Industry 5.0; higher education.

Reference to this paper should be made as follows: Stanelytė, D. 2026. Recognising employees' competences through verifiable micro-credentials: aligning higher education and employers' needs in the digital era. *Entrepreneurship and Sustainability Issues*, 13(3), 143–158. <http://doi.org/10.9770/n3433346968>

JEL Classifications: M53, M54, O31

Additional disciplines: educology; information and communication

1. Introduction

Digitalisation, automation and the green transition are changing how companies and entrepreneurs create value, organise work and compete in markets. Under the Industry 5.0 and Society 5.0 paradigms, technology is increasingly expected to support human-centred, sustainable development, not only productivity gains (Hossain & Purdy, 2024; Atay et al., 2025). Production and service systems become more data-intensive and integrated along digital value chains (Voulgaridis et al., 2022; Chuma & Ngoepe, 2025). For employers this means a growing dependence on employees who combine specialised technical competences with transversal skills such

* This research was funded by INVESTech Innovation Vocational Excellence and Sustainability in Tech PROJECT REF NO. 101143958. ERASMUS-EDU-2023-PEX-COVE Programme

as problem solving, collaboration and continuous learning. Evidence from Industry 5.0 initiatives and regional upskilling programmes shows that large segments of the workforce must be reskilled or upskilled in short, targeted learning cycles closely linked to the workplace (Doyle-Kent & Shanahan, 2022; Doyle-Kent et al., 2022; Pinto et al., 2024). The ability to identify, verify and deploy suitable competences has therefore become a strategic condition for innovation, entrepreneurship and sustainable business development.

Labour markets, however, still rely mainly on traditional credentials and self-reported CVs as signals of capability. Cross-country studies indicate that when the level and field of education are aligned with occupational structures, workers enjoy higher earnings and lower unemployment risk; when alignment is weak, both individuals and firms bear the cost of mismatch (Vogtenhuber, 2018; DiPrete & Chae, 2023). Conventional degrees describe programmes in broad terms and provide limited insight into what an employee can actually do in specific digital or green transition tasks. This information gap is even more pronounced for competences gained through short courses, employer-led training, non-formal programmes and informal workplace learning. For entrepreneurs and managers seeking to build agile teams, it is difficult to judge the level, scope and reliability of such learning, even when it is crucial for new business models in areas such as smart manufacturing, circular economy or data-driven services.

In response, higher education institutions (HEIs), training providers and companies are experimenting with more flexible, modular forms of learning. Short, demand-driven technical programmes and micro-courses are used to tailor skills to sectoral needs and to support lifelong learning in applied fields (Mena-Guacas et al., 2023; Pinto et al., 2024). Micro-credentials and digital badges package these learning experiences into focused units that can stand alone or be stacked into larger qualifications. The literature highlights that such micro-credentials can make learning more responsive to employer demand, support career transitions and widen access to upskilling opportunities beyond full-degree pathways (Shanahan & Organ, 2022; Yılık, 2025). Sector-specific examples show how micro-credentials are co-designed with industry to support life-long learning for urban energy transitions and renewable energy ecosystems (De Rosa et al., 2024) or to personalise professional learning pathways (Vordenberg et al., 2024; Fan et al., 2024).

At the same time, the rapid expansion of micro-credential initiatives raises governance and recognition issues. HEIs emphasise robust pedagogy, clear learning outcomes and authentic assessment (Shanahan & Organ, 2022; Catenazzi et al., 2025), while employers need simple, comparable and trustworthy signals that can be integrated into recruitment, internal mobility and competence management processes. Without common principles for describing and verifying micro-credentials, there is a risk of fragmentation: many small certificates that are difficult for employers to interpret and therefore have limited business value. Existing research on digital badges and holistic competencies shows that, in practice, evidence of specific competency achievement is often embedded in final degrees and remains invisible, and that systems for documenting and reporting such competencies are fragmented and not well aligned with labour-market needs (Chan & Chen, 2022). This underlines the importance of moving from generic claims about “skills” to verifiable, portable and employer-readable competences. Technological developments offer tools to address these problems but also introduce new layers of complexity. Open digital badges based on recognised data models allow structured information about learning outcomes, assessment and evidence to be attached to a visual credential (Catenazzi et al., 2025). Emerging wallet-based and blockchain-enabled solutions promise tamper-evident, privacy-aware and portable credentials that employees can share directly with employers across organisational and national boundaries (Alsobhi et al., 2023; El Koshiry et al., 2023; Gottlieb et al., 2024). New digital “wallets” allow employees to share secure, hard-to-fake credentials with employers with a single click, regardless of which institution issued them. Interoperability frameworks and reference models stress the need for aligned semantics and verification processes if credentials are to move reliably between HEI systems, learner wallets and employer platforms (Chukowry et al., 2021; Perisic et al.,

with those developed in non-formal and informal learning, treating them as parts of a single portfolio that must be visible and trustworthy for employers. It asks three questions: (1) what requirements do employers and entrepreneurial firms have for the way competences are described and verified in digital credentials; (2) how can HEIs design micro-credentials and digital badges so that these requirements are met across formal, non-formal and work-based learning; and (3) what minimum data and governance rules are needed for a verifiable micro-credential profile that is both technically interoperable and economically meaningful for companies.

This article is unique in two respects. First, building on the call for systematic documentation and recognition of competencies in higher education (Chan & Chen, 2022; Catenazzi et al., 2025), it explicitly reframes micro-credentials as a strategic instrument for entrepreneurship, human-capital management and sustainable business development, rather than as a purely educational innovation. It integrates insights from Industry 5.0 skills demand, competence mismatch research and digital credential technologies to propose a three-layer model (pedagogical–assessment, technological–verification, recognition–policy) that is oriented to employer decision-making. Second, it translates this model into a practical, stepwise profile for verifiable micro-credentials that can be read by employers, aggregated at company level and used to support skills-based recruitment, internal mobility and continuous upskilling strategies aligned with green and digital transitions (Shanahan & Organ, 2022; Alsobhi et al., 2023; De Rosa et al., 2024; Atay et al., 2025). In doing so, the paper positions micro-credentials at the interface between education and business, contributing to the economics, management and entrepreneurship focus of the journal.

2. Concepts and theoretical foundations

2.1. Definitions

Micro-credential. A micro-credential is a record of focused learning achievement, awarded by a trusted provider after assessment against defined standards; it has standalone value and can contribute to larger qualifications, with description elements that include learning outcomes, assessment type, quality assurance, and—where possible—ECTS and EQF level (Zain, 2023; Catenazzi et al., 2025).

Open badge (digital badge). An open badge is a digital credential consisting of a visual image and embedded metadata—such as issuer, description, criteria, evidence, recipient, validity and revocation—that is human-readable, machine-verifiable, cryptographically signed, and tamper-evident under the 1EdTech Open Badges specification (Catenazzi et al., 2025).

Stacking. Stacking refers to combining several short learning experiences or badges so they either remain standalone or accrue into a larger micro-credential or qualification pathway (Shanahan et al., 2022; Zain, 2023).

Portfolio and wallet. A learner portfolio is an e-portfolio that aggregates study documents and evidence of learning for sharing in academic processes (Gottlieb et al., 2024). A credential wallet is a learner-controlled application that stores and manages issued credentials—often alongside institutional wallets for issuers—supporting collection, presentation, and verification across contexts (Gottlieb et al., 2024).

Interoperability. Interoperability is the capacity of credentials to be issued, read, and verified across platforms through common data models and formats such as 1EdTech Open Badges, the W3C Verifiable Credentials (VC) data model, and the European Learning Model (ELM), enabling portability and machine processing (Catenazzi et al., 2025).

Verification models. In issuer-hosted verification, systems like Blockcerts publish an issuer profile and public key used to validate signatures and revocation status of a credential stored on or referenced by a public ledger (Gottlieb et al., 2024). In decentralised verification, learners present W3C VCs linked to Decentralised Identifiers (DIDs), reducing reliance on centralized authorities and enabling privacy-preserving proofs within trust

Scope note. These definitions are aligned with the article’s focus on a narrative, concept-centred review of micro-credentials, digital badges, and verifiable credentials in higher education and VET, ensuring consistent terminology across the manuscript (Shanahan et al., 2022; Catenazzi et al., 2025).

2.2. Ecosystem: learner–higher education institution–employer

Learner. Learners seek clear, portable, and recognised evidence of competence; they value transparency, ownership, and the ability to aggregate and present evidence through an e-portfolio or credential wallet across platforms (Perisic et al., 2023; Catenazzi et al., 2025).

Higher education institution (HEI). HEIs design learning that is outcomes-based, use authentic assessment, ensure quality assurance, and issue verifiable badges aligned with qualification levels and credit systems (De Rosa et al., 2024; Catenazzi et al., 2025).

Employer. Employers signal in-demand competences and expect intelligible artefacts (e.g., code, prototypes, reports) and verifiable badges; coordinated interaction among the three actors narrows the study–work gap (Shanahan & Organ, 2022; De Rosa et al., 2024).

Interaction logic. The ecosystem operates as a coherent chain: labour-market signals → formulation of learning outcomes → authentic assessment → portfolio evidence → badge with metadata → verification → recognition. In practice, outcome-aligned, team-based and experiential tasks generate employer-readable artefacts that can be referenced in badge metadata and presented from a learner portfolio/wallet (Shanahan & Organ, 2022; Perisic et al., 2023; Catenazzi et al., 2025).

Industry 5.0 anchoring. Human-centricity, sustainability, and resilience imply “visible” evidence that is machine-readable and verifiable. Aligning learning outcomes and assessment criteria with evidence URLs produces tamper-evident artefacts that employers can automatically read and check, setting up Section 4.1 where employer needs are mapped to the minimum metadata profile and interoperability requirements (Chukowry, 2021; El Koshiry, 2023; Catenazzi, 2025).

2.3. Standards and recognition

Metadata and traceability. Badge metadata must encode, at minimum, the learning outcomes (LO)→assessment→evidence chain plus credit and level, so that credentials align with qualification systems and credit practice (e.g., ECTS, EQF) and remain machine-readable across platforms (Catenazzi, 2025).

Quality assurance. Combine internal (programme) and external (institutional/partner) QA: publish transparent assessment criteria, an evidence typology, and validation procedures to enable cross-institution comparability of badges (Shanahan & Organ, 2022; De Rosa, 2024). As for implications, adopting nationwide and regional frameworks, using digital stacking tools, and operating on decentralized blockchain-like verification technologies to realize the recognition and quality assurance of micro-credentials would best serve the interests of the micro-credential stakeholders, including higher education itself as a scientific and institutional actor (Yılık, 2025).

Interoperability guidelines. Follow open, **heterogeneous** interoperability principles so that data

Stacking and institutional recognition. From an employer’s perspective, the information on credit volume (ECTS) and qualification level (EQF) in each badge works like a “scale” and “difficulty label” for the competence signal. When several badges share compatible levels and credits, higher education institutions can group them into larger micro-credentials or even components of degree programmes. For companies, this stacking reduces micro-fragmentation: HR specialists can interpret a bundle of badges as a coherent block of study rather than a set of isolated short courses. Machine-readable metadata, based on Open Badges, W3C Verifiable Credentials and the European Learning Model, make it possible to check automatically who issued the badge, at what level and on what kind of evidence. This lowers the cost and risk of relying on micro-credentials in recruitment and internal promotion decisions.

Data protection and lifecycle. Apply data minimisation and lifecycle controls, especially when evidence includes assessment artefacts; expose links (evidence URLs) while keeping personal data and sensitive files under appropriate access policies.

Bridge to Sections 4.3 and 6. Section 4.3 details the minimum field set, and Section 6 translates these standards into HEI implementation steps.

The standards-to-recognition pathway connects assessment and learning objectives to transferable, verifiable credentials, as illustrated in Figure 1.

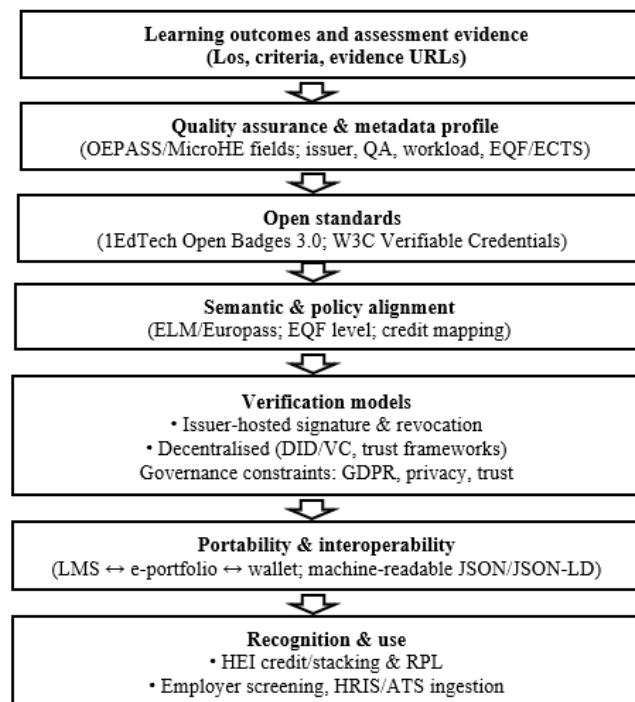


Figure 1. Standards-to-recognition stack for micro-credentials
(Open Badges 3.0 ↔ W3C Verifiable Credentials, aligned with ELM/EQF)

3. Methodology

3.1. Review type

A narrative, concept-centred review was conducted, focusing on the micro

3.2. Search strategy and data sources

Evidence base. The review draws exclusively on a pre-specified corpus of 30 peer-reviewed articles selected for this study, predominantly hosted on ScienceDirect/Elsevier and spanning 2016–2025. No additional records were sought beyond this set.

Scope and language. English-language journal articles (research and review).

Screening within the set. Items were screened for relevance to at least one of the target concepts: *micro-credential / microcredential*; *open badge / digital badge*; *interoperability / W3C Verifiable Credentials*; *portfolio / wallet*; *verification / blockchain*; *ECTS / EQF*; *Industry 4.0 / 5.0*. All 30 met inclusion aims for the concept-centred synthesis; therefore, counts of excluded items and PRISMA flow were not applicable to this pre-specified corpus.

Data handling. A standard extraction form captured bibliographic details, context/type, key definitions, ecosystem roles, LO→assessment→evidence elements, badge metadata, interoperability aspects (LMS–e-portfolio–wallet flows and semantics), verification type (issuer-hosted / decentralised) and conditions, quality/recognition, and pedagogy. Extraction and coding procedures are detailed in Sections 3.5–3.7, with audit-trail materials noted in Section 3.8.

3.3. Inclusion and exclusion criteria

Inclusion

- **Topical relevance:** direct coverage of at least one target concept: micro-credentials / digital (open) badges; LO→assessment→evidence chain; interoperability (Open Badges 3.0, W3C Verifiable Credentials, ELM/Europass); verification (issuer-hosted vs decentralised, blockchain); quality/recognition (ECTS, EQF); pedagogy in short courses.
- **Publication type and quality:** peer-reviewed journal articles (research or reviews) with accessible full-text PDF.
- **Context:** higher education and/or VET; employer-recognition or labour-market alignment considered a plus.
- **Language and period:** English; 2016–2025.
- **Fit to synthesis:** provides conceptual, methodological, or technical material usable for the narrative, concept-centred integration.

Exclusion

- Out of scope (e.g., digital badges with no assessment/evidence linkage; blockchain papers without education/credentialing focus).
- Non-peer-reviewed items (editorials, opinion pieces, short notes) or inaccessible full text.
- Duplicates or near-duplicates.
- Languages other than English; contexts limited to K-12 without transferability to HE/VET.

Application to the corpus. The criteria were applied to the pre-specified set of 30 peer-reviewed PDFs selected for this study; all 30 met inclusion aims for the concept-centred synthesis. No additional records were sought beyond this set; consequently, PRISMA flow counts are not applicable to this design. Screening and eligibility checks used the extraction form in Section 3.5 and coding categories in Section 3.6 to ensure consistency with the study's objectives.

3.4. Screening flow

This review used a pre-specified corpus of 30 peer-reviewed articles. A

3.5. Data extraction

A standardized extraction form was used for each source to capture:

- bibliographic details and study context/type;
- key definitions;
- ecosystem roles;
- LO→assessment→evidence elements;
- badge metadata (e.g., LO_ID, learningOutcomes, assessmentCriteriaURL, evidenceURL, creditECTS, levelEQF, issuer, issueDate/validThrough, badgeClass/assertion, signature/publicKey, verification);
- interoperability aspects (LMS–e-portfolio–wallet flows and semantics);
- verification type (issuer-hosted / decentralised) and conditions;
- quality/recognition (QA, transparency, benchmarking);
- pedagogy (principles for short courses).

Extraction fields are aligned with the minimal interoperability profile specified in Section 4.3 to ensure machine-readable traceability from learning outcomes to recognition and consistent, cross-institution comparability.

3.6. Coding scheme

A deductive–inductive coding approach was applied. An initial codebook was seeded from the conceptual domains of the review and iteratively refined during pilot coding to ensure alignment with the extraction fields in Section 3.5 and the results structure in Sections 4.1–4.7. Unit of analysis: statement or subsection fragment. Multiple coding was allowed where passages spanned several domains; disagreements were addressed through iterative re-review and consensus, with codebook updates recorded in the audit trail (see Section 3.8).

Codebook categories (a–g):

- Ecosystem (learner–HEI–employer interactions and labour-market signals);
- LO–assessment–evidence chain (intended/achieved LOs, authentic assessment, portfolio artefacts);
- Badge metadata (minimum profile fields and traceability requirements);
- Interoperability (LMS–e-portfolio–wallet flows; semantic/data-model alignment);
- Verification (issuer-hosted vs decentralised); keys, signatures, revocation, trust frameworks);
- Quality / recognition (QA, transparency, ECTS/EQF mapping, stackability, inter-institution recognition);
- Pedagogy (short courses) (experiential/team-based tasks that generate employer-readable artefacts).

Traceability and outputs. Codes were mapped to the extraction fields (Section 3.5) to maintain machine-readable traceability from learning outcomes to recognition and to the results subsections (4.1–4.7) for thematic synthesis. The coding matrix (categories × sources) is provided in Table 1 as documentation of coverage and triangulation.

Table 1. Coding matrix (categories × sources)

	a) Ecosystem (learner–HEI– employer)	b) LO– assessment– evidence chain	c) Badge metadata (minimum profile)	d) Interoperability (LMS–e- portfolio–wallet; semantics)	e) Verification (issuer-hosted vs decentralised)	f) Quality / recognition (ECTS/E
--	--	--	--	--	---	--

3.7. Analysis procedure

A staged procedure was applied within the pre-specified 30-article corpus:

1. **Pilot coding (n=3):** the initial codebook was checked against sample sources to refine code definitions and examples, ensuring alignment with Section 3.5 fields and the planned results structure (Sections 4.1–4.7).
2. **Full-corpus coding (n=30):** statements and subsection fragments were coded deductively–inductively across seven domains (ecosystem; LO–assessment–evidence; badge metadata; interoperability; verification; quality/recognition; pedagogy). Multiple coding was allowed where passages spanned several domains.
3. **Thematic synthesis:** codes were grouped into themes and subthemes and cross-walked to the LO→assessment→evidence→badge chain and to interoperability/verification requirements.
4. **Model consolidation:** themes were integrated into a three-layer model (pedagogical–assessment; technological–verification; recognition–policy) and into the minimum interoperability profile used in Section 4.3.
5. **Quality checks:** an audit-style review verified that each substantive claim was supported by multiple sources and that codebook updates were recorded and traceable (see Section 3.8).

3.8. Reliability and transparency

Audit trail. The audit trail comprises the coding matrix (categories × sources), the codebook with versioned updates, and a decision log documenting notable coding changes; materials are available on request to support verification of the analytic path.

Reproducibility. Study parameters (keywords, database, time window, inclusion criteria) are specified in Sections 3.2–3.3 to enable replication using the same pre-specified corpus design.

Bias mitigation. Multiple coding was permitted; potential disagreements were resolved by iterative re-review and consensus. Agreement thresholds of $\geq 85\%$ overlap or Cohen's $\kappa \geq 0.70$ were treated as acceptable for risk-prone passages.

3.9. Ethics and limitations

Ethics. The review analysed published, peer-reviewed documents only; no human participants or personal data were involved. Sources consisted of publicly available PDFs selected a priori, and analysis focused on conceptual and technical content relevant to micro-credentials, badges, interoperability, and verification. Institutional ethics approval was not required for this document-based synthesis.

Limitations.

This review synthesises a pre-specified corpus of 30 peer-reviewed journal articles drawn from defined databases and a 2016–2025 window; grey literature and non-English studies may therefore be under-represented. The analysis is concept- and method-oriented and does not prescribe or empirically trial specific IT stacks or API-level implementations, and no meta-analytic effect sizes are estimated. Generalisation beyond higher education and VET contexts should be made cautiously, as long-term economic outcomes (e.g., ROI, employment effects) were not quantitatively evaluated. Finally, results are bounded by rapidly evolving credential standards (Open Badges 3.0 / W3C VC / ELM/EQF), which may necessitate periodic updates as ecosystems mature.

4. Results: thematic synthesis

4.2. The LO → assessment → evidence → badge chain

Learning outcomes are operationalised through authentic assessment; the resulting artefacts are referenced in the badge metadata to make the LO→assessment→evidence link explicit and machine-verifiable. Issuance follows Open Badges 3.0 with mappings to W3C Verifiable Credentials and ELM/EQF, enabling automated checks of issuer, level and credit and supporting stackability into modules or programme components (Catenazzi et al., 2025; De Rosa et al., 2024). Verification proceeds via issuer-hosted signature/revocation for institutional contexts or decentralised DID/VC models where cross-institution trust, tamper-evidence and long-term availability are required (Chukowry et al., 2021; El Koshiry et al., 2023; Gottlieb et al., 2024). This chain ensures end-to-end traceability from intended outcomes to recognised, employer-relevant credentials across systems.

4.3. Minimal badge profile (Open Badges 3.0 ↔ W3C VC ↔ ELM/EQF)

This subsection specifies the minimum machine-readable metadata required to ensure portability and verification across LMS, e-portfolio, and wallet contexts. Fields map to 1EdTech Open Badges 3.0, align with W3C Verifiable Credentials, and indicate ELM/EQF semantics for recognition.

Table 2. Minimum badge profile (fields, purpose, example)

Name	Purpose	Example
LO_ID	links the badge to a specific learning outcome	LO-ENG6-001
learningOutcomes	machine-readable description of achieved outcomes	"Builds a working prototype..."
assessmentCriteriaURL	public rubric/criteria reference	https://example.org/...
evidenceURL	link(s) to portfolio artefacts	https://example.org/...
creditECTS	workload for stacking/recognition	3 ECTS
levelEQF	qualification level where applicable	EQF 6
issuer	institutional issuer identifier	KVK – Faculty of Technology
issueDate / validThrough	issuance and (if applicable) validity	2025-05-01 / –
badgeClass	badge class/type	BadgeClass: Prototype Builder
assertion	unique assertion identifier	urn:uuid:1f2e-...
signature / publicKey	cryptographic signature and key reference	JWS / did:key:z6Mkh...
verification	verification method	Issuer-hosted / decentralised registry.

Implementation notes.

- The profile **must be JSON/JSON-LD**, signed, and consistently validated (signature, public key, revocation/verification endpoint).
- Exposed fields enable **automated checks** (issuer, level, credit, evidence) and **stackability** into modules or programme components.
- Choice of **verification method** depends on scale, privacy,

- **Durability.** Short retention → issuer-hosted; long-term availability → decentralised.
 - **Privacy & regulation.** Restrictive policies (GDPR constraints on evidence) → minimise on-chain content; keep **evidence URLs** off-chain while registering verifiable assertions.
 - **Cost & latency.** Low/medium → issuer-hosted is sufficient; higher resilience/trust needs → decentralised is justified.
 - **Sensitivity of artefacts.** Public metadata only → issuer-hosted suffices; artefacts driving credential decisions → prefer decentralised proofs with selective disclosure.
- This logic maintains alignment with Table 2 and ensures that verification choices preserve portability and recognition requirements across institutions.

4.6. Pedagogical considerations for short courses

Authentic, team-based assignments should produce employer-readable artefacts (e.g., code, prototypes, reports) that are explicitly referenced in badge metadata via evidence URLs. Outcomes must be assessable with transparent rubrics (assessmentCriteriaURL) so the LO → assessment → evidence link is auditable. Short courses benefit from concise outcome statements, calibrated workload (ECTS), explicit EQF levels where applicable, and portfolio practices that foreground artefacts rather than only grades. This ensures that pedagogical design directly feeds the minimal badge profile and later verification/recognition steps. One of the main findings is that short-term courses are primarily designed for experiential learning, and memory-related activities commonly used in traditional training are not typically included in short-term courses (Mena-Guacas et al., 2023).

4.7. Quality assurance and recognition

Quality assurance combines internal (course/programme QA) and external (institution/partner) checks to support comparability. A concise QA checklist should confirm: (i) declared outcomes and public rubrics; (ii) evidence typology and links; (iii) conformance with Open Badges 3.0 / W3C VC; (iv) mapping to ELM/EQF and clear ECTS workload; (v) working verification (signature, key, revocation endpoint); and (vi) data protection controls over evidence. Recognition proceeds when machine-readable metadata allow automated checks of issuer, level, credit, and evidence, enabling stacking into modules/components and portability across institutions and employer systems. However, over 70% of the reviewed studies did not issue certificates or badges for participants (Wang & Hu, 2025).

5. Integrated model and decision rules

5.1. Consolidated model

The integrated model combines three interacting layers that link intended learning to verifiable recognition across systems:

- **Pedagogical–assessment layer.** Clearly formulated learning outcomes are operationalised through transparent rubrics and authentic tasks that generate employer-readable artefacts (e.g., code, prototypes, reports). These artefacts are referenced in badge metadata via evidence links, preserving auditable traceability from LO to assessment and evidence (see Sections 4.1–4.2).
- **Technological–verification layer.** Minimum machine-readable metadata are issued in Open Badges 3.0 (JSON-LD) with mappings to W3C Verifiable Credentials and semantic anchors to ELM/EQF. Verification follows either issuer-hosted signature/revocation **or** decentralised DID/VC models depending on scale, privacy and durability needs (Sections 4.3–4.5).
- **Recognition–policy layer.** When level (EQF) and workload (ECTS) are exposed in metadata and evidence is resolvable, credentials can be stacked into modules or programme components and recognised across institutions

Mappings and conformance.

- Encode badges as Open Badges 3.0 and map to W3C VC to enable cryptographic verification and selective disclosure where required.
- Expose ELM/EQF semantics (level, workload) to support stacking and cross-institution recognition.
- Keep artefacts referenced via evidence URLs; avoid embedding personal data in signed payloads.

Validation and governance.

- Enforce signature checks, public-key resolution and revocation status at verification time (issuer-hosted or decentralised).
- Apply data-minimisation and lifecycle controls (GDPR): publish rubrics and evidence links transparently while restricting access to sensitive artefacts.
- Choose issuer-hosted verification for institutional contexts; prefer decentralised (DID/VC with registry) when cross-institution trust, tamper-evidence and long-term availability are required.

This minimum profile operationalises the three-layer model in 5.1 and maintains end-to-end machine-readable traceability from learning outcomes to recognised credentials across systems.

5.3. Decision rules and implementation steps

This subsection summarises the decision logic for applying the integrated model.

Verification choice.

- Issuer-hosted signature/revocation is suitable for internal or limited-partner use, lower cost, and short-to-medium retention.
- Decentralised (DID/VC with registry) is preferred for cross-institution recognition, tamper-evidence, and long-term availability.

Data model alignment. Every credential must conform to Open Badges 3.0 (JSON-LD) with mappings to W3C VC and semantic anchors to ELM/EQF, exposing the minimum fields from Table 2 (e.g., LO_ID, learningOutcomes, assessmentCriteriaURL, evidenceURL, creditECTS, levelEQF, issuer, signature/publicKey, verification).

HEI implementation sequence (pointer). (1) align LOs and rubrics; (2) declare the minimum metadata; (3) enable signing and verification; (4) pilot on a short course; (5) formalise recognition with partners. See Section 6 for the institutional, 8–10-step plan.

5.4. Bridge to institutional guidelines

Data-flow view. The integrated model in Section 5.1 describes the horizontal flow from learning outcomes (LO) → assessment → evidence → badge → verification → recognition across LMS–e-portfolio–wallet contexts.

Why this matters for implementation. The flow clarifies which fields must be present in the badge payload (Table 2), where verification occurs (issuer-hosted **vs** decentralised), and how metadata enable stacking and cross-institution recognition. This bridge sets up Section 6 (Guidelines for HEI implementation), where the model is operationalised through concrete steps, QA checks, and risk controls.

6. Guidelines for HEI implementation

This section translates the outcomes→assessment→evidence→badge→verification→recognition chain into

4. Design the credential and minimum profile. Configure Open Badges 3.0 (JSON-LD) with the core fields in Table 2 (e.g., LO_ID, creditECTS, levelEQF, evidenceURL, issuer, signature/publicKey, verification) and mappings to W3C VC/anchors to ELM.
5. Enable issuer-hosted verification. Deploy signing and revocation checks to ensure immediate institutional verification and tamper-evidence.
6. Prepare decentralised registration. Integrate DID/VC-based options (registry or trusted third party) for cross-institution trust and long-term availability.
7. Integrate with LMS and e-portfolio/wallet. Automate issuance, viewing, and evidence linkage across LMS ↔ e-portfolio ↔ wallet.
8. Establish QA and stacking rules. Define internal QA, evidence typology, and how compatible micro-credentials stack into modules or programme components.
9. Set up inter-institution recognition. Align metadata with ELM/EQF and formalise recognition protocols with partners.
10. Monitor and evaluate. Track uptake, employer feedback, administrative cost, and outcomes (e.g., employability/ROI) to iterate the model.

6.2. Risks and mitigation

As summarised in Table 3, the key risks for HEI deployment—along with their potential impact and preventive/corrective measures—are aligned with the step-by-step plan in Section 6.1.

Table 3. Risks and mitigation

Risk / challenge	Potential impact	Preventive / corrective measures
System fragmentation across HEIs	Incompatible data formats; non-portable badges	Sectoral standardisation on Open Badges 3.0 and ELM; shared profiles and validators
Unclear ROI / employer value	Slow adoption; weak recognition	Transparent rubrics; real evidence in portfolios; periodic impact reviews with employers
Privacy and data protection	Personal-data exposure	GDPR compliance; data minimisation; keep artefacts behind evidenceURL with access control
Limited technical capacity	Implementation errors; data loss	Staff training; shared guidelines; sandbox/testing environments and helpdesk
Divergent partner recognition	Uneven acceptance of credentials	Inter-institution agreements; ECTS/EQF mapping; automated validation tools
Low ecosystem trust	Slow rollout; stakeholder scepticism	Public verification endpoints; certified signatures; third-party attestations
Excessive data retention	Security risk; higher costs	Metadata lifecycle control; minimise payload content; clear revocation policies

These controls should be embedded in governance and QA (policies, procedures, and vendor SLAs) and monitored during pilots and rollout. Use Table 3 as a pre-flight checklist alongside the minimum badge profile in Table 2; unresolved high-impact items should block release until mitigated. Finally, the main challenges educators encountered were related to the platform, time, resources, awareness, and micro mindset (Fan et al., 2024). Practical recommendations include national digital standards, micro-credential training programmes and industry–government–academia partnerships. (Siriwardhana, Moehler, & Fang, 2025). Enterprise credential spear-phishing using look-alike domains can evade common email defenses, which motivates layered mitigations such as domain/IP whitelisting, DKIM/SPF checks, and domain-similarity detection (Al-Hamar et al., 2021). Blockchain technology provides a decentralized, distributed, and secure environment to ensure security and privacy preservation (Alsobhi et al., 2023). Short, online, self-paced courses (“micro-courses”) are

6.3. Summary

HEI deployment should be phased: build internal QA and issuer-hosted verification first, then extend to decentralised registration and inter-institution recognition. Maintaining a tight link from LO and assessment to evidenceURL and the fields in Table 2 ensures machine-readable traceability and portability across systems and employer contexts.

7. Discussion

7.1. Positioning relative to prior work

The synthesis extends earlier treatments that either catalogued digital badges and European transparency instruments or focused narrowly on blockchain verification. Here, the pedagogical–assessment layer (LOs, authentic assessment, portfolio artefacts) is explicitly linked to technological verification and recognition-policy layers, closing the LO → assessment → evidence → badge → verification → recognition loop. By specifying a minimum interoperability profile and decision rules for issuer-hosted versus decentralised verification, the model moves beyond descriptive accounts toward an actionable, institution-ready pathway (Shanahan & Organ, 2022; Catenazzi et al., 2025; El Koshiry et al., 2023; Gottlieb et al., 2024). Evidence from comparative labour-market research shows that credentials continue to carry independent signalling power beyond measured skills; in coordinated market economies, the higher-education credential effect exceeds the standardised skill effect across countries (Vogtenhuber, 2018). This underlines the importance of making credential information as transparent and competence-based as possible. In a different context, Young’s (2011) analysis of institutional separation and space in teacher education shows how programme design, organisational arrangements and physical settings shape which competences become visible and recognised. The model proposed in this article responds to these insights by using micro-credentials and portfolios to surface competences that might otherwise remain implicit and to encode them in forms that can be read by both higher education institutions and employers.

7.2. Practical implications for HEIs and employers

For HEIs, aligning outcomes, public rubrics and evidence URLs with Open Badges 3.0 (mapped to W3C VC and anchored to ELM/EQF) enables machine-readable traceability and stackability. Governance should require signing, key resolution and revocation checks; the choice between issuer-hosted and decentralised verification follows privacy, scale and durability needs. For employers, portable badges carrying verifiable links to artefacts (code, prototypes, reports) reduce screening uncertainty and support skills-based selection and progression. At the same time, empirical work on the returns to education shows that the premium for a college degree is accumulative, multidimensional and multigenerational, and should be considered at the household level (Alon & Mcdossi, 2025). This suggests that verifiable micro-credentials will complement rather than replace traditional degrees by adding transparent, competence-level information to an already powerful credential signal. To make this complementarity effective, educational institutions and organisations should offer flexible learning opportunities, such as online courses, micro-credentials and apprenticeships, to support professionals in acquiring new skills and staying relevant in the changing job market (Pinto et al., 2024).

7.3. Scope and limitations

Findings derive from a concept-centred synthesis of 30 peer-reviewed articles; no additional records were sought. The approach is conceptual–methodological rather than an IT blueprint, and it does not quantify economic effects (e.g., ROI) or long-term labour-market outcomes. Consequently, generalisation beyond HE/VET contexts should be cautious, and updates may be required as Open Badges/W3C VC/ELM evolve.

7.4. Directions for research and policy

Future work should test cross-institution recognition at scale (shared validators, DID/VC registries), measure outcomes for learners and employers, and refine selective-disclosure patterns for privacy-sensitive evidence. Policy efforts should standard

Conclusions

This review synthesised recent work on micro-credentials to connect the LO → assessment → evidence → badge → verification → recognition chain into an actionable pathway for higher education and employers. The resulting three-layer model—pedagogical–assessment, technological–verification, and recognition–policy—keeps employer-readable artefacts at the centre while aligning credential data with Open Badges 3.0, mappings to W3C Verifiable Credentials, and ELM/EQF semantics (see Figure 1).

A minimum interoperability profile (see Table 2) specifies the core machine-readable fields—linking LOs, rubrics and evidence URLs to issuer identity, credit (ECTS), level (EQF), signature/public key, and verification method—so that credentials are portable across LMS, e-portfolios and wallets, and stackable into modules or programme components. This profile enables automated checks of issuer, level, credit and evidence, improving comparability and recognition across institutions.

Verification follows issuer-hosted signature/revocation for institutional contexts or decentralised DID/VC arrangements when cross-institution trust, tamper-evidence and long-term availability are required. The decision rules ensure privacy-aware, cost-appropriate and scalable assurance without embedding sensitive artefacts in signed payloads (evidence remains referenced via links).

For implementation, the ten-step plan in Section 6 operationalises governance, data modelling and systems integration, while Table 3 provides risk-mitigation controls to be embedded into QA and policy (e.g., standardisation on Open Badges 3.0/ELM, GDPR-aligned data minimisation, key management and revocation, inter-institution recognition protocols). Institutions can phase adoption: establish internal QA and issuer-hosted verification first, then extend to decentralised registration and partner recognition.

Overall, the model offers a coherent route from intended learning to verifiable, portable recognition—grounded in open standards and geared to Industry 5.0’s human-centric skills agenda—thereby reducing ambiguity for HEIs and employers and providing a stable foundation for sector pilots and future evaluation.

References

- Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise credential spear-phishing attack detection. *Computers & Electrical Engineering*, 94, 107363. <https://doi.org/10.1016/j.compeleceng.2021.107363>
- Alon, S., & Mcdossi, O. (2025). Inherent advantage: The multidimensional and cumulative nature of intergenerational associations in degree attainment. *Research in Social Stratification and Mobility*, 99, 101090. <https://doi.org/10.1016/j.rssm.2025.101090>
- Alsobhi, H. A., Alakhtar, R. A., Ubaid, A., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, 265, 110238. <https://doi.org/10.1016/j.knosys.2022.110238>
- Atay, S., Terzi Müftüoğlu, C., Gülmez, N., & Ş

Chukowry, V., Nanuck, G., & Sungkur, R. K. (2021). The future of continuous learning–Digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, 2, 355-361. <https://doi.org/10.1016/j.gltp.2021.08.026>

Clayback, K. A., LoCasale-Crouch, J., & Alamos, P. (2024). A pilot study of a micro-course to promote positive teaching practices and prevent exclusionary discipline in early childhood. *Early Childhood Research Quarterly*, 67, 182-190. <https://doi.org/10.1016/j.ecresq.2023.12.010>

De Rosa, M., Glumac, O., Bianco, V., & Pallonetto, F. (2024). A micro-credential approach for life-long learning in the urban renewable energy sector. *Renewable Energy*, 228, 120660. <https://doi.org/10.1016/j.renene.2024.120660>

DiPrete, T. A., & Chae, J. (2023). Coordinated markets, school-to-work linkages, and labor market outcomes in Europe. *Research in Social Stratification and Mobility*, 87, 100840. <https://doi.org/10.1016/j.rssm.2023.100840>

Doyle-Kent, M., & Shanahan, B. W. (2022). The development of a novel educational model to successfully upskill technical workers for Industry 5.0: Ireland a case study. *IFAC PapersOnLine*, 55(39), 425-430. <https://doi.org/10.1016/j.ifacol.2022.12.072>

Doyle-Kent, M., O'Neill, B., Shanahan, B. W., Organ, J., Doyle, L., O'Neill, S., Costello O., Donnelly, N. (2022). A research cluster's vision for a pilot factory in the South East Technological University of Ireland. *IFAC PapersOnLine*, 55(39), 159-164. <https://doi.org/10.1016/j.ifacol.2022.12.028>

El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M. Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain: Research and Applications*, 4, 100165. <https://doi.org/10.1016/j.bcra.2023.100165>

Fan, X., Wei, X., Lewis

Voulgaridis, K., Lagkas, T., Angelopoulos, C. M., & Nikoletseas, S. E. (2022). IoT and digital circular economy: Principles, applications, and challenges. *Computer Networks*, 219, 109456. <https://doi.org/10.1016/j.comnet.2022.109456>

Wang, C., & Hu, X. (2025). Teacher online professional learning: A systematic literature review. *Educational Research Review*, 49, 100727. <https://doi.org/10.1016/j.edurev.2025.100727>

Zain, S. (2023). Micro-credentials: need to be benchmarked across institutions. In *Benchmarking library, information, and education services* (Chap. 20). Elsevier. <https://doi.org/10.1016/B978-0-323-95662-8.00026-6>

Funding: This research was funded by INVESTech Innovation Vocational Excellence and Sustainability in Tech PROJECT REF NO. 101143958. ERASMUS-EDU-2023-PEX-COVE Programme.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy concerns.

Daiva STANELYTĖ is a Lecturer at Klaipėdos valstybinė kolegija / Higher Education Institution, Lithuania. Research interests: energy systems; smart grids; smart device technologies; digitalization.

ORCID ID: <https://orcid.org/0000-0002-9623-6653>

Copyright © 2026 by author(s). Publishing rights by Entrepreneurship and Sustainability Center

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access