

# Badges and Digital Credentials in Higher Education

## What They Are, When to Use Them, and How They Work Together

### ABOUT THIS GUIDE

**Audience:** Non-technical staff at universities - academic managers, registry offices, quality assurance teams, international offices.

**Purpose:** To provide a clear, authoritative reference on what badges and digital credentials are, how they differ, and how they can work together. This guide does not advocate for any specific technology or vendor.

**Format:** EUNIS SIG practical guide, companion to existing SIG outputs.

**Published by:** EUNIS Special Interest Group - Mobility & Digital Credentials · Version 0.3 · June 2026

## 1. Why This Guide Exists

The ecosystem of digital credentials has grown rapidly, and the terminology is genuinely confusing - even among specialists. Universities across Europe are being asked to make consequential decisions about platforms, processes, and integrations, often without a clear map of the landscape.

Three specific problems motivate this guide:

- Vocabulary fragmentation. The same words - badge, credential, microcredential - are used differently by different communities, standards bodies, and policy documents. Misalignment at the vocabulary level leads to misaligned decisions.
- A false binary. Many institutions treat Open Badges and European Digital Credentials as competing alternatives. They are not: they solve different problems, serve different purposes, and can complement each other.
- Infrastructure pressure without conceptual clarity. The regulatory clock is running. eIDAS 2.0, the EUDI Wallet, and the SDG/OOTS framework create real deadlines. Institutions need to act, but acting well requires understanding before implementing.

This guide is intended as a companion to the discussion papers the EUNIS SIG Mobility & Digital Credentials already produces - accessible enough for non-technical staff, grounded enough to inform strategic and operational decisions. It does not advocate for any specific technology, platform, or vendor.

### How to use this guide

Section 2 establishes the shared vocabulary. Sections 3–4 cover Open Badges and EDC in depth. Section 5 analyses the trust spectrum. Section 6 is the decision framework. Section 7 covers the combination model. Section 8 maps implications to specific university functions.

Sections 9–10 provide recommendations and resources. Appendix A contains seven use case scenarios comparing Open Badges and EDC in practice; Appendix B is the glossary.

## 2. A Shared Vocabulary: Five Concepts to Keep Separate

Before comparing standards and platforms, it is necessary to establish a shared vocabulary. Five concepts are routinely conflated, with real consequences for institutional decisions.

### 2.1 Digital Badge

A digital badge is a visual digital element that represents participation or achievement, typically within a closed ecosystem such as a learning management system or a gamification layer. It may carry no structured metadata beyond a name and an image, is not portable outside the system that issued it, and implies no verification mechanism.

A digital badge is the most basic form of digital recognition - analogous to a sticker or a stamp. It communicates meaning to those who understand the context, but carries no independent trust or verifiability.

### 2.2 Open Badge

An Open Badge is a digital badge that conforms to the 1EdTech Open Badges standard. The word 'open' refers to interoperability and portability, not to the absence of criteria. An Open Badge carries structured, machine-readable metadata (issuer, recipient, criteria, evidence) that travels with the image and can be verified by any party.

The key distinctions from a simple digital badge: it is portable across compliant platforms, it is verifiable (at least at the level of issuer and recipient), and it is not locked into any single vendor ecosystem.

### 2.3 Credential

A credential is a formal attestation issued by a trusted authority confirming a qualification, competence, or right. Credentials exist in physical and digital forms: a paper diploma, a campus card, and a signed certificate are all credentials, as is a cryptographically signed digital record. What defines a credential is not its format but the institutional authority and trust behind it. A credential is a container for trust.

### 2.4 Digital Credential

A digital credential is a credential issued, stored, and shared digitally. In its strong form - aligned with the W3C Verifiable Credentials Data Model (W3C-VCDM) - it is tamper-evident and cryptographically verifiable without contacting the issuer.

A scanned PDF diploma is digital in a trivial sense. A W3C-VCDM credential with a qualified digital signature is a digital credential in the full sense: independently and offline verifiable.

### 2.5 Microcredential

A microcredential is a type of learning achievement - not a format or a size of document. It is defined by the EU Council Recommendation (2022):

**EU Council Recommendation on microcredentials (2022)**

"A micro-credential is a record of learning outcomes acquired following a small volume of learning, assessed against transparent criteria, and shareable digitally."

Required elements: learner identity · stated learning outcomes · workload (ECTS or notional hours) · EQF/NQF level · assessment method and criteria · quality assurance reference · issuer information

**The two layers of any educational credential**

Every educational credential - diploma, transcript, or microcredential - is built on two inseparable layers. Each is necessary; neither is sufficient on its own. The EU Council Recommendation (2022) codifies both layers explicitly and with mandatory force for microcredentials, making them the clearest reference point for institutions designing any credential:

| Layer                    | Content                                                                                                                                      | Consequence if missing                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Pedagogical / Regulatory | Stated outcomes, assessed performance, QA reference, EQF level, ECTS workload, issuer information. Defined by the EU Council Recommendation. | Without this layer: not a microcredential. It is training. No framework will recognise it. |
| Technical / Trust        | How the record is structured, signed, and shared. Implemented via EDC (ELM + qualified signature + wallet).                                  | Without this layer: no cross-border interoperability or independent verification.          |

*Note: the pedagogical and regulatory layer exists independently of format. A paper diploma has learning outcomes, an EQF level, and a quality assurance reference - even if none of these are machine-readable. What the technical layer adds is not the content itself but the ability to verify, share, and process that content digitally and across borders.*

**KEY POINTS**

*Short course ≠ microcredential.*

*Without stated outcomes, formal assessment, and a quality assurance reference, a learning activity is training - however valuable. Technology cannot substitute for the pedagogical layer.*

**2.6 The Core Distinctions**

| Concept       | Dimension                                             | Portability                           | Verifiability                 |
|---------------|-------------------------------------------------------|---------------------------------------|-------------------------------|
| Digital badge | Visual element in a closed system                     | None - locked to issuing platform     | None                          |
| Open Badge    | Portable, structured digital badge (1EdTech standard) | High - interoperable across platforms | Basic to cryptographic (v3.0) |
| Credential    | Formal attestation of qualification or competence     | Depends on format                     | Depends on format             |

| Concept            | Dimension                                                          | Portability               | Verifiability                      |
|--------------------|--------------------------------------------------------------------|---------------------------|------------------------------------|
| Digital credential | Credential issued, stored, shared digitally (W3C-VCDM strong form) | High - holder-controlled  | Cryptographic - offline verifiable |
| Microcredential    | Type of learning achievement (EU Council Rec. 2022) - not a format | Depends on implementation | Requires EDC for EU conformance    |

**KEY POINTS**

*A digital badge and an Open Badge are not the same thing.*

*A digital badge is a visual element in a closed system. An Open Badge is a portable, structured, verifiable digital badge conforming to the 1EdTech standard.*

*A microcredential is defined by pedagogical rigour, not size or format. For EU conformance it requires EDC.*

*For cross-border recognition, only credentials with legal trust and cryptographic verification qualify.*

### 3. Open Badges: What They Are and What They Do

Open Badges is an open technical standard for digital badges, originally developed by Mozilla and now maintained by the 1EdTech Consortium. Machine-readable metadata travels with the badge: issuer, recipient, criteria, and evidence.

#### 3.1 What makes Open Badges open

- Interoperable across platforms - the standard is openly specified and not tied to any vendor
- Learner-controlled - badges can be stored in any compliant wallet or portfolio chosen by the recipient
- Freely implementable - any party can issue or receive compliant badges

#### 3.2 What Open Badges can do

- Provide structured, interoperable recognition of learning and achievement
- Enable verification of issuer and recipient (basic in v2.1; cryptographic in v3.0)
- Support engagement, motivation, and visibility in learning journeys
- Allow fast deployment with low governance overhead
- Recognise non-formal and informal learning, extracurricular activities, skills, and professional development
- In v3.0: function as a W3C Verifiable Credential (with appropriate issuer infrastructure)

#### 3.3 What Open Badges cannot guarantee

- Institutional recognition under EU administrative frameworks
- Legal validity under eIDAS 2.0
- Conformance with the EU Council Recommendation on microcredentials
- Cross-border interoperability in the EU recognition chain
- Persistence of value if the issuing or hosting platform changes

### 3.4 OB v3.0: the important change

Open Badges version 3.0 aligns with the W3C Verifiable Credentials Data Model. This means a v3.0 badge can technically be a verifiable credential. This matters for combination scenarios (Section 7). However, technical compatibility with W3C-VCDM does not in itself confer eIDAS legal standing, integration with EU trust frameworks, or the semantic fields required by the European Learning Model.

### 3.5 Where Open Badges add most value

| Use case                                             | Suitability   | Notes                                                     |
|------------------------------------------------------|---------------|-----------------------------------------------------------|
| Skills visibility and professional portfolios        | High          | Strong social sharing mechanics; widely used by employers |
| Engagement and motivation during learning            | High          | Milestones, participation, progress indicators            |
| Non-formal and informal learning recognition         | High          | Low governance overhead; flexible criteria                |
| Extracurricular activities, volunteering, leadership | High          | Fast to deploy; no QA requirement                         |
| Professional development and CPD                     | High          | Used in many national CPD frameworks                      |
| Formal assessed microcredentials (EU Rec. 2022)      | Non-compliant | Missing ELM semantic fields - see Section 4               |
| Cross-border recognition and Erasmus workflows       | Low           | Not part of EU recognition infrastructure                 |

### 3.6 What Open Badges demands from institutions

Open Badges have substantially lower technical requirements than EDC, but they are not cost-free:

| Requirement                      | Notes                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuing infrastructure           | Integration with LMS or standalone issuing service. Governed process for who can issue and under what criteria.                                              |
| Assertion hosting                | Badge assertions must be hosted and remain accessible for verification. Contractual control required if hosted by a third party.                             |
| Criteria and evidence definition | Each badge type requires documented criteria. Without this, badges carry no meaningful information and will not be taken seriously.                          |
| Expiry and revocation policy     | Institutions need a policy on when badges expire and under what circumstances they are revoked. This is a governance decision, not just a technical setting. |
| Data processing agreement        | If a third-party platform is used, a GDPR-compliant DPA is required. Learner data (name, email, achievement) is personal data.                               |

| Requirement                       | Notes                                                                                                                                         |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Governance of issuing authority   | Define who in the institution can authorise a new badge type and issue badges in the institution's name.                                      |
| Branding and recognition strategy | Badges issued without a communications strategy are rarely claimed or shared. Define how learners will be informed and motivated to use them. |

**KEY POINTS**

*Open Badges are not plug-and-play.*

*The technical entry point is low, but the governance entry point is the same as for any recognised form of institutional recognition.*

*Institutions that treat badge issuance as a purely technical decision end up with badges that are neither claimed nor trusted.*

## 4. European Digital Credentials: What They Are and What They Do

A European Digital Credential (EDC) is a digitally signed, cryptographically verifiable record of a learning achievement. It is structured using the European Learning Model (ELM) and verifiable without contacting the issuer. It is designed from the ground up for cross-border recognition. How it is delivered and stored depends on the lineage: EDCI/Europass uses file-based delivery; DC4EU/EBSI is wallet-native.

### 4.1 The four dimensions of an EDC

| Dimension       | What it means                                                                                                                                                                                                   | Why it matters                                                                                            |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Structure       | European Learning Model (ELM): issuer, holder, learning outcomes, workload (ECTS), EQF level, assessment method, quality assurance reference.                                                                   | Shared semantics across Member States. Machine-readable comparability.                                    |
| Trust           | Digitally signed. Issuer registered in national/EU trust framework. Cryptographic verification. Aligned with eIDAS regulation.                                                                                  | Independent verification without contacting the issuer. Legal standing under EU law.                      |
| Portability     | Depends on lineage.<br>EDCI/Europass: JSON-LD file, optionally stored in Europass.<br>DC4EU/EBSI: wallet-native - stored in EUDI Wallet or equivalent. Both are holder-controlled and independently verifiable. | The learner controls their credential. Wallet storage is native to DC4EU/EBSI; optional in EDCI/Europass. |
| Legal alignment | Aligned with eIDAS 2.0, EQF, ESG, Bologna framework. Does not grant legal status alone - issuer accreditation still required.                                                                                   | Enables formal recognition processes, Lisbon Convention workflows, and EMREX integration.                 |

## 4.2 The European Learning Model (ELM)

ELM is the semantic backbone of EDC. It defines the ontology - the shared vocabulary of concepts and relationships - that makes credentials machine-readable and comparable across institutions and jurisdictions. Key fields that ELM defines and Open Badges does not:

- EQF level - referenced as an IRI to the Publications Office controlled vocabulary
- ECTS credit points - with framework reference and numeric range constraints
- Assessment (provenBy) - mandatory in microcredentials; the key semantic differentiator
- Awarding body and jurisdiction - with eIDAS legal identifier for the issuer
- Quality assurance reference - mandatory for microcredential conformance
- Learning achievement specification - subject area (ISCED-F), learning mode, competence references (e.g. ESCO)

This is why a microcredential conforming to the EU Council Recommendation cannot be implemented as an Open Badge: the required fields simply do not exist in the Open Badges specification.

## 4.3 Two EDC lineages - same regulation, different architecture

There are two technically distinct lineages operating under the same EU regulatory framework. Choosing between them is a strategic and architectural decision - not a question of preference.

|                         | Europass / EDCI                                                                                   | eIDAS 2.0 / EBSI / DC4EU                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Status                  | Established - deployed across 40+ countries today                                                 | Future-proof - wallet-native, EUDI-aligned                                                     |
| Technical base          | EDCI JSON-LD, qualified seals for signing                                                         | W3C-VCDM, DID/EBSI, QTSP/PSB-issued credentials                                                |
| Storage / Wallet        | Credential delivered as JSON-LD file; optional storage in Europass repository (not wallet-native) | Wallet-native: EUDI Wallet (Member State-issued) or equivalent; also non-EUDI wallets for EAAs |
| Trust model             | Centralised: Europass trusted issuer list; classical PKI                                          | Hybrid: classical PKI + verifiable data registries (EBSI) + trusted lists                      |
| Revocation / Suspension | Limited mechanisms                                                                                | StatusList2021 or equivalent; supports both revocation and suspension                          |
| eIDAS alignment         | eIDAS 1.0 qualified seals                                                                         | eIDAS 2.0 QEAA / PubEAA; SDG/OOTS compatible                                                   |
| Deployment readiness    | Production                                                                                        | Pilot - approaching production                                                                 |

### KEY POINTS

*These lineages are not competing - they serve different timelines and use cases. Europass/EDCI for deployment today. DC4EU/EBSI/eIDAS 2.0 for the long-term wallet paradigm.*

*The choice is determined by the data transfer model - not by preference.*



## 4.4 Data transfer models

The choice between EDC lineages is largely determined by the data transfer pattern:

| Model                                       | Description                                                                                                                                                           | EDC lineage                                      |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| LE → NP<br>(Legal Entity to Natural Person) | Institution issues a credential directly to the student. The holder stores it and shares as needed.<br>Example: diploma, transcript, microcredential.                 | Both Europass/EDCI and DC4EU/EBSI work           |
| LE → LE<br>(Legal Entity to Legal Entity)   | Institution shares data directly with another institution, without the citizen as intermediary.<br>Example: partner university verifying enrolment for Erasmus.       | Typically SDG/OOTS, Europass/EDCI, or direct API |
| LE → NP → LE<br>(Citizen-mediated)          | The citizen receives a credential, stores it in their wallet, and presents it to a relying party.<br>Example: student presents EducationalID at a partner university. | DC4EU / EBSI / eIDAS 2.0 wallet paradigm         |

## 4.5 What EDC demands from institutions

- Registration as a trusted issuer in the relevant trust registry
- Decentralised Identifier (DID) management and key infrastructure (for DC4EU/EBSI)
- Compliance with ELM v3.2 - all semantic fields correctly populated
- Schema registration and reference to controlled vocabularies (EQF, ISCED-F, ESCO)
- Qualified digital signatures aligned with eIDAS requirements
- Wallet integration for credential delivery
- Governance definition: awarding authority, QA references, GDPR data controller designation
- Ongoing maintenance: key rotation, revocation lists, schema versioning

### KEY POINTS

*Governance before technology - every time.*

*Legal entity, awarding authority, QA framework, and data controller designation must all be defined before any technical implementation begins.*

*Every technical shortcut taken before the legal and governance framework is defined creates rework.*

## 5. The Trust Spectrum

Understanding the relative trust levels of different credential formats is essential for matching the format to the use case.



| Format                         | Verification mechanism                                    | Legal standing (EU)      | Suitable for formal recognition? |
|--------------------------------|-----------------------------------------------------------|--------------------------|----------------------------------|
| PDF Certificate                | None - visual inspection only                             | None                     | No                               |
| Open Badge (OB v2.1)           | Hosted assertion - URL-based                              | None                     | No                               |
| Open Badge (OB v3.0)           | Optional cryptographic signature (W3C-VCDM compatible)    | None inherent            | Limited - no ELM fields          |
| EDC / Europass (EDCI)          | Cryptographically signed; issuer in Europass trusted list | eIDAS 1.0 qualified seal | Yes                              |
| EDC + EUDI Wallet (DC4EU/EBSI) | Cryptographic + EBSI trust registry + QTSP/PSB signature  | eIDAS 2.0 QEAA / PubEAA  | Yes - highest assurance          |

### 5.1 EDC is necessary but not sufficient

An EDC provides technical trust and interoperability. Legal validity additionally requires an accredited issuer, a functioning governance framework, and regulatory alignment. A cryptographically signed credential issued by a non-accredited body is technically valid and legally meaningless.

### 5.2 Open Badges carry real social value - with a caveat

Badges have genuine economic value in talent ecosystems. However, this value is platform-dependent, not framework-dependent. It can diminish or disappear when platforms change their policies, are acquired, or cease to operate.

### 5.3 The interoperability pillar order

A critical principle from the European Interoperability Framework (EIF): the four pillars must be addressed in order. Technology is always the last layer:

| Pillar       | Content                                                                                      | Consequence if skipped                                             |
|--------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 1. Legal     | Aligned legislation, policies, and agreements. The prerequisite.                             | No legal validity; credentials not recognised across borders.      |
| 2. Business  | Aligned processes, responsibilities, and governance.                                         | Governance gaps; no clear awarding authority or accountability.    |
| 3. Semantic  | Shared meaning. ELM ensures that a 'learning outcome' in Spain means the same as in Finland. | No cross-border comparability; credentials become local artefacts. |
| 4. Technical | APIs, data formats, protocols. The last layer - not the first.                               | Technical solutions that cannot deliver cross-border value.        |

## 6. Decision Framework: When to Use What

The choice of credential format should follow purpose, not preference. Three questions structure the decision:

1. Is cross-border institutional recognition required?
2. Is legal standing under eIDAS required?
3. Who is the primary consumer - a person's professional profile, or an institutional process?

### 6.1 Use case matrix

| Use case                                      | Open Badge      | EDC               | Recommended          |
|-----------------------------------------------|-----------------|-------------------|----------------------|
| Informal participation / engagement           | ✓ Well suited   | Optional          | Badge                |
| Skills visibility / portfolio                 | ✓ Good          | ✓ Better          | EDC + optional badge |
| Formal microcredential (EU Council Rec. 2022) | ✗ Non-compliant | ✓ Required        | EDC only             |
| Transcript / diploma                          | ✗ Poor fit      | ✓ Strong          | EDC only             |
| Cross-border recognition                      | ✗ Not supported | ✓ Strong          | EDC only             |
| Erasmus / mobility workflows                  | ✗ Not supported | ✓ Strong          | EDC only             |
| Regulated profession evidence                 | ✗ Poor fit      | ✓ Strong          | EDC only             |
| Engagement during learning (milestones)       | ✓ Well suited   | Not needed        | Badge                |
| Social sharing alongside formal credential    | ✓ Well suited   | Underlying record | Badge + EDC          |

#### KEY POINTS

*A microcredential in the sense of the EU Council Recommendation (2022) cannot be implemented as an Open Badge alone.*

*The required fields - EQF level, ECTS workload, assessment method, QA reference, issuer identity - have no native semantic equivalent in the Open Badges specification. These fields are defined by the European Learning Model (ELM), which only EDC implements.*

*Open Badge = how the learner shares and communicates the achievement.*

*EDC = how the institution accredits it and society recognises it.*

### 6.2 Decision map: trust and semantic rigour

The diagram below positions the main credential formats along two axes: level of trust and independent verification (horizontal) and level of semantic rigour and comparability (vertical).

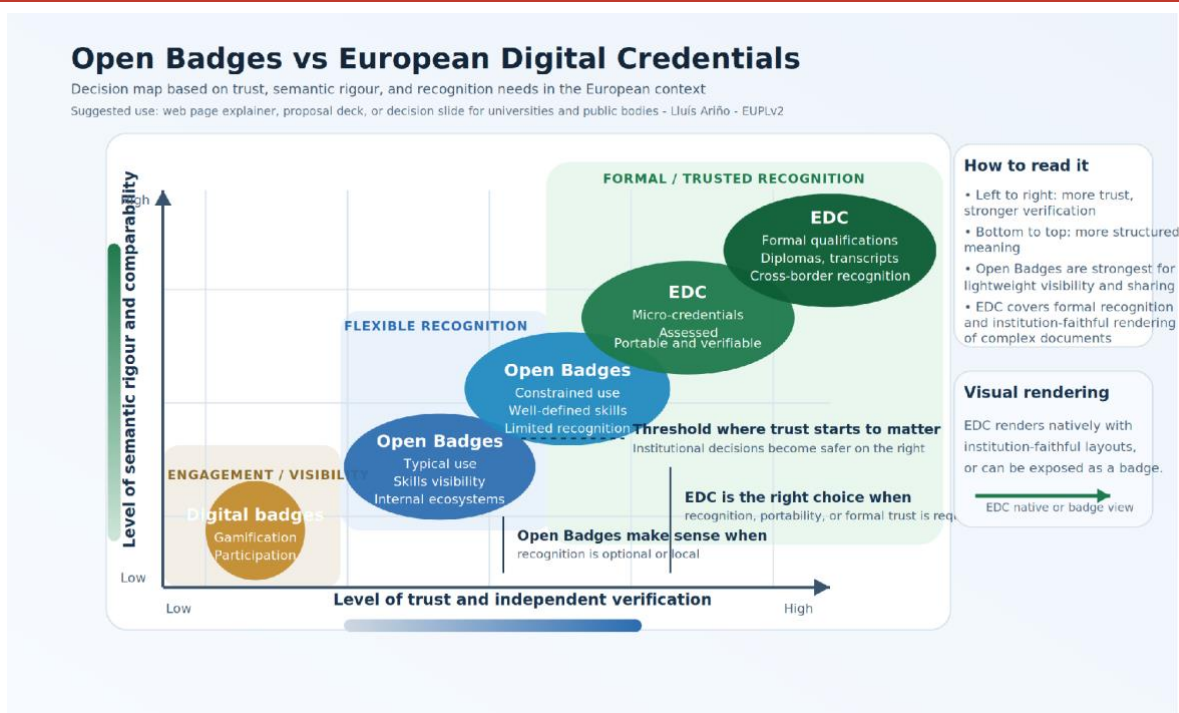


Figure 1. Open Badges vs European Digital Credentials - decision map by trust and semantic rigour. Source: EUNIS SIG (EUPLv2)

## 6.3 Choosing between EDC lineages

| Question                                        | Europass / EDCI        | DC4EU / EBSI / eIDAS 2.0 |
|-------------------------------------------------|------------------------|--------------------------|
| Do you need to deploy formal credentials today? | Yes - production-ready | Not yet - pilot phase    |
| Is the citizen the intermediary?<br>(LE→NP→LE)  | Partial support        | Primary design target    |
| Do you need EUDI Wallet compatibility?          | No                     | Yes                      |
| Is eIDAS 2.0 QEAA required?                     | No - eIDAS 1.0 seals   | Yes                      |
| Is long-term cross-border wallet use the goal?  | Transitional solution  | Strategic target         |

## 7. The Combination Model: Badges and EDC Together

Open Badges and EDC are not mutually exclusive. They serve different purposes for different audiences and can be designed to work together within a coherent institutional architecture. Understanding why requires first looking at the technical foundation they share.

### 7.1 The shared technical foundation: W3C Verifiable Credentials Data Model

Both EDC (DC4EU/EBSI lineage) and Open Badges v3.0 are built on the W3C Verifiable Credentials Data Model (W3C-VCDM). This shared foundation is what makes combination architectures technically feasible - and also what makes it necessary to understand why technical compatibility alone does not make the two standards equivalent for recognition purposes.

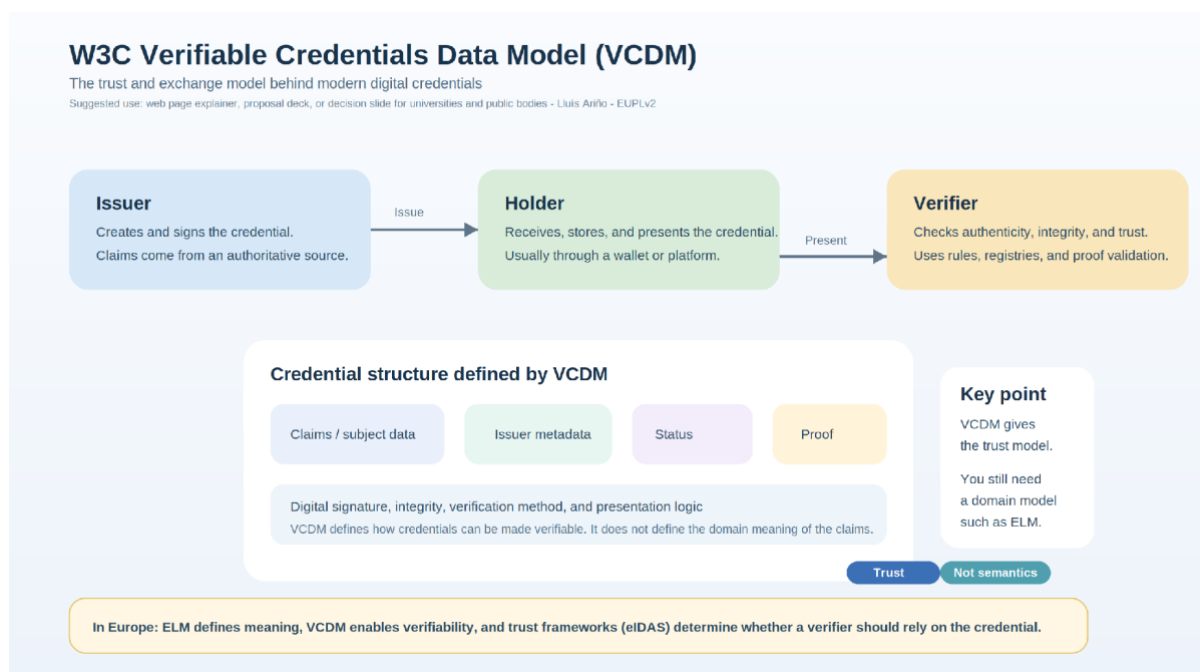


Figure 3. W3C Verifiable Credentials Data Model - the shared technical foundation for EDC (DC4EU/EBSI) and Open Badges v3.0. Source: EUNIS SIG (EUPLv2)

The model defines three roles: the issuer (who creates and signs the credential), the holder (who stores and presents it), and the verifier (who checks it independently without contacting the issuer). Both EDC and OB v3.0 implement this triangle. The difference is what sits on top: EDC adds the ELM semantic layer, which is what makes it suitable for formal European recognition. W3C-VCDM gives both standards the same trust plumbing; ELM gives EDC the domain meaning.

#### KEY POINTS

*W3C-VCDM gives the trust model. ELM gives the meaning. eIDAS gives the legal framework.*

*Technical compatibility between OB v3.0 and EDC does not mean semantic or legal equivalence.*

## 7.2 The layered architecture

| Layer                               | Role                                                                                                               | Standard                             |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| Layer 0 - Academic source systems   | Student information system, diploma registry, QA registry, identity systems. The authoritative data source.        | Institutional (SIS, LMS, QA systems) |
| Layer 1 - Trust and governance      | Trusted issuer registration, qualified signatures, eIDAS identity framework, awarding authority governance.        | EDC / eIDAS 2.0 / EBSI               |
| Layer 2 - Verifiable credential     | Signed, machine-readable, independently verifiable formal record.                                                  | EDC (ELM + W3C-VCDM)                 |
| Layer 3 - Experience and engagement | Social sharing, portfolio visibility, motivation during learning, labour market signalling. Optional but valuable. | Open Badge (optional)                |

Badge = view. EDC = evidence. Trust = governance. Each layer has a defined role; none substitutes for another.

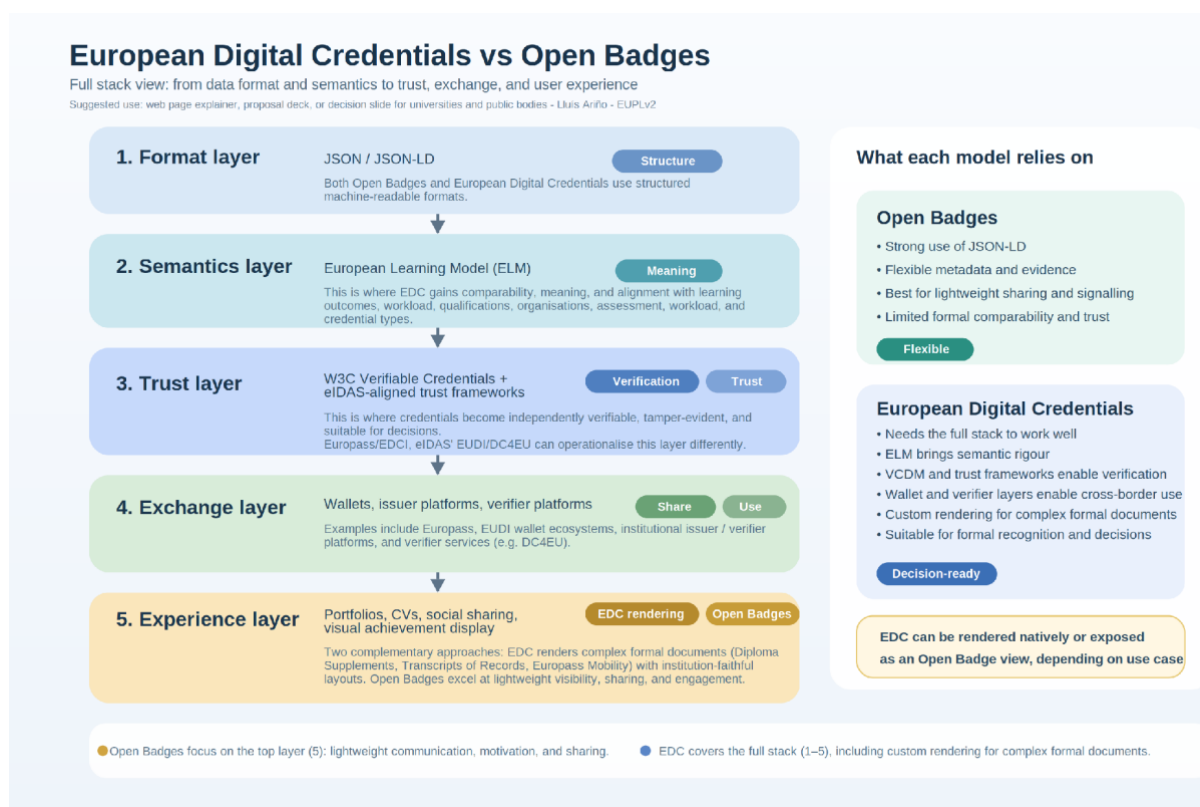


Figure 2. European Digital Credentials vs Open Badges - full stack view. Source: EUNIS SIG (EUPLv2)

## 7.3 Practical combination scenarios

| Scenario                                       | How it works                                                                                                                                               | Who benefits                                                |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| EDC microcredential + social badge             | Issue an EDC microcredential as the formal institutional record. Issue an Open Badge referencing the EDC for the learner's professional profile.           | Registry (EDC) + learner visibility (badge)                 |
| Engagement layer + formal record at completion | Use Open Badges during learning for milestones, participation, and skills. Issue an EDC at programme completion.                                           | Learner motivation during + institutional recognition after |
| Alliance badge over institutional EDC          | Each partner institution issues its own EDC. The alliance issues a shared Open Badge for the joint programme - no legal entity at alliance level required. | Alliance branding without governance complexity             |
| Badge as a window into a credential            | Issue a lightweight badge that surfaces and links to the verifiable EDC underneath.                                                                        | Both communities: labour market + institutional recognition |

## 7.4 Technical note on OB v3.0 and EDC compatibility

There is not yet an established interoperability profile between Open Badges v3.0 and EDC in production implementations. The harmonisation of standards is still ongoing. Documenting emerging practices, identifying gaps, and contributing to the standards debate are natural areas of future exploration for university networks and communities of practice such as this SIG.

## 8. Practical Implications by University Function

| University function             | Implications                                                                                                                                                                                                                                                                   |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registry / Student Records      | EDC requires integration with trusted issuer infrastructure, DID management, and qualified signatures - a realistic timeline of 12–24 months for production readiness. Open Badges can be issued via LMS integrations with much lower overhead. Plan these on separate tracks. |
| Quality Assurance               | EDC microcredentials require ELM conformance: assessed, scoped, stackable, and QA-referenced. Open Badges impose no such requirements - flexibility and risk. The QA office must define which activities qualify for each.                                                     |
| International / Mobility Office | EDC is the format for Lisbon Recognition Convention digital workflows, EMREX data exchange, and Erasmus+ digital processes. Open Badges are not currently part of that infrastructure.                                                                                         |
| IT / Systems                    | EDC demands DID management, schema registration, wallet integration, and qualified signatures. Open Badges have a much lower technical entry point. Do not conflate the timelines or the workstreams.                                                                          |
| Communications / Marketing      | Open Badges have strong social sharing mechanics. EDC credentials are primarily for official processes. A combined strategy - EDC as the formal record, badge as the social artefact - captures the value of both.                                                             |
| Legal / Data Protection         | EDC under eIDAS 2.0: holder-controlled storage, selective disclosure, defined GDPR roles. Open Badges via third-party platforms: DPA required, data residency review. The DPO should be involved from the governance design phase.                                             |

## 9. Key Recommendations

Six recommendations for university leaders, managers, and policy professionals:

1. **Clarify purpose before format.** The question is not 'badge or EDC?' - it is 'what outcome does this recognition need to achieve, and for whom?'
2. **Do not wait for EDC infrastructure to be fully mature before acting on Open Badges.** They solve different problems. The Open Badge ecosystem is production-ready today.
3. **Align with the EU Council Recommendation before choosing a platform.** If you intend to issue microcredentials, define outcomes, assessment criteria, and QA reference first. The pedagogical layer cannot be retrofitted.
4. **Choose your EDC lineage deliberately.** Europass/EDCI for deployment today; DC4EU/EBSI/eIDAS 2.0 for the long-term wallet paradigm. Know which data transfer model your primary use case requires.



5. **Plan for both formats from the same learning record.** Build processes capable of outputting either format. Avoid architecture lock-in.
6. **Governance before technology - every time.** Before any platform or standard is chosen, formalise what a credential means in your institution: its required content, legal basis, and academic value. Review internal regulations, workflows, and policies that were written assuming physical formats and identify any that inadvertently block or complicate digital issuance. Define your legal entity, awarding authority, QA framework, and GDPR data controller designation. Technology cannot substitute for governance, and governance cannot be retrofitted around a platform that has already been chosen.

## 10. Resources and Further Reading

---

### Standards and specifications

- 1EdTech Open Badges v3.0 specification - <https://www.imsglobal.org/spec/ob/v3p0/>
- W3C Verifiable Credentials Data Model 2.0 - <https://www.w3.org/TR/vc-data-model-2.0/>
- European Learning Model (ELM) v3.2 and browser - <https://europa.eu/europass/elm>

### Policy and regulatory frameworks

- EU Council Recommendation on microcredentials (2022) - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:243:TOC>
- eIDAS 2.0 Regulation (EU) 2024/1183 - [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L\\_202401183](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183)
- European Qualifications Framework (EQF) - <https://europa.eu/europass/eqf/>
- European Standards and Guidelines for Quality Assurance (ESG) - <https://www.enqa.eu/esg/>
- European Interoperability Framework (EIF) - [https://ec.europa.eu/isa2/eif\\_en](https://ec.europa.eu/isa2/eif_en)

### Infrastructure and implementation

- Europass / EDC documentation - <https://europa.eu/europass/en>
- EBSI (European Blockchain Services Infrastructure) - <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI>
- DC4EU educational pilot and sectoral EAA catalogue - <https://github.com/dc4eu/educational-pilot/>
- EUDI Wallet Architecture Reference Framework - <https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation>
- EMREX - <https://emrex.eu/>

### EUNIS SIG outputs

- EUNIS SIG Mobility & Digital Credentials - <https://eunis.org/task-forces/mobility-and-digital-credentials-special-interest-group/>



## Appendix A - Use Cases and Institutional Scenarios

This appendix presents seven scenarios comparing how Open Badges and European Digital Credentials perform across real university use cases. Each scenario follows a common structure: institutional context, a step-by-step journey for each standard, where Open Badges break down, what EDC enables, and the key takeaways - including the specific value for university alliances.

The scenarios are intended as a practical complement to the decision framework in Section 6. Institutions can map their own use cases to the most relevant scenarios and use them as a basis for planning.

| Scenario                                               | Primary question                                                             | Key finding                                                         |
|--------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------|
| A.1 Formal Microcredential Issuance                    | Can a short-course credential be formally recognised across EU institutions? | Open Badges non-compliant with EU Council Rec. - EDC required       |
| A.2 Credit Recognition and ECTS Transfer               | Can a receiving institution automate credit evaluation?                      | Only EDC provides structured, automatable data                      |
| A.3 Erasmus Mobility and Cross-Border Recognition      | Does the credential integrate with EU mobility infrastructure?               | Only EDC connects to Erasmus Without Paper and EMREX                |
| A.4 Admissions to Postgraduate Programme               | Can the credential support a legally defensible admissions decision?         | Open Badges provide claims; EDC provides verified evidence          |
| A.5 Diploma and Degree Issuance                        | Is the credential permanently and independently verifiable?                  | Only EDC is verifiable without issuer involvement, with revocation  |
| A.6 Employer Verification                              | Can HR systems verify the credential automatically?                          | Only EDC enables machine-readable, fraud-proof verification         |
| A.7 Alliance-Internal Recognition and Skills Portfolio | Can the alliance create a single coherent learning record across partners?   | Only EDC with a shared profile creates genuine academic integration |

### A.1 Formal Microcredential Issuance

#### Context

A university issues a short-course credential (15–60 hours) to a student completing a structured learning programme. The credential must be usable for recognition, credit transfer, or employment.

Actors: Issuing university · Student / learner · Receiving institution or employer

## Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                        | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Instructor defines badge criteria in free text</li> <li>2. Badge issued and delivered to student wallet or profile</li> <li>3. Student shares badge link or image</li> <li>4. Receiver inspects badge metadata manually</li> <li>5. No structured data to automate evaluation</li> </ol> | <ol style="list-style-type: none"> <li>1. Institution maps course to ELM data model</li> <li>2. Nine EU-required elements captured: outcomes, workload, EQF level, assessment, QA reference, issuer</li> <li>3. EDC signed and issued to student wallet</li> <li>4. Student shares credential from wallet</li> <li>5. Receiver verifies cryptographically, reads structured data</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>No mandatory learning outcomes, workload, EQF level, assessment method, or QA reference. Two badges from different institutions are not comparable. Receiver cannot automate evaluation. Trust level: informal recognition only.</i></p>                                                  | <p><b>What EDC enables</b></p> <p><i>Credential is machine-readable, comparable across institutions, and aligned with the EU Council Recommendation (2022). QA is verifiable. Assessment method is explicit. Trust level: formal microcredential, EU-compliant.</i></p>                                                                                                                     |

### Key takeaways

- Open Badges record that something happened. EDC attests what was learned, how it was assessed, and who guaranteed the quality.
- Only EDC meets the nine required elements of the EU Council Recommendation - without them, the credential cannot be formally recognised.
- Receiving institutions can automate pre-recognition with EDC. With Open Badges, every case requires manual academic judgement.

#### Alliance value

A shared EDC profile across alliance partners ensures all institutions issue comparable microcredentials - enabling automatic mutual recognition within the alliance.

### Scenario 1 of 7

## A.2 Credit Recognition and ECTS Transfer

#### Context

A student completes a module at University A (Spain) and requests recognition of ECTS credits at University B (Germany). The receiving institution must evaluate the equivalence.

Actors: Student · Sending university · Receiving university academic registrar

## Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                    | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Student presents badge from sending institution</li> <li>2. Register reviews badge: free-text criteria, optional evidence links</li> <li>3. Register contacts sending institution to clarify content</li> <li>4. Manual academic committee review initiated</li> <li>5. Decision made case-by-case, weeks or months later</li> </ol> | <ol style="list-style-type: none"> <li>1. Student shares EDC from wallet</li> <li>2. Receiving registry resolves credential cryptographically</li> <li>3. Structured fields read directly: ECTS credits, EQF level, learning outcomes, assessment method, QA body</li> <li>4. Automated pre-recognition logic applied against equivalence rules</li> <li>5. Decision supported by structured evidence, not institutional goodwill</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>No standard ECTS workload field. No guaranteed learning outcomes format. No external QA reference. Each case is treated as unique - no automation possible. High administrative cost on both sides. Trust level: manual, slow, inconsistent.</i></p>                                                                                  | <p><b>What EDC enables</b></p> <p><i>ECTS workload, EQF level, and learning outcomes are explicit and standardised. Pre-recognition can be partially automated. Administrative burden reduced on both sides. Decision is auditable. Trust level: structured, comparable, automatable.</i></p>                                                                                                                                                |

## Key takeaways

- Open Badges require the receiving institution to trust the issuer's reputation. EDC requires it to trust a cryptographic proof anchored in EU infrastructure.
- ECTS workload is a structured field in EDC. In Open Badges it is either absent or buried in free text - unprocessable by any system.
- Automation is only possible with EDC. Open Badge-based recognition will always require human intervention, which limits scale.

### Alliance value

With shared EDC profiles, partner universities can define common recognition rules in advance and apply them automatically - turning mobility into a process, not a negotiation.

## Scenario 2 of 7

## A.3 Erasmus Mobility and Cross-Border Recognition

### Context

A student applies for an Erasmus+ mobility placement. The host institution must evaluate the student's prior learning and agree on a Learning Agreement before departure.

Actors: Student · Home institution · Host institution · National Erasmus office

## Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                                                                            | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Student assembles portfolio of badges</li> <li>2. Host institution reviews each badge individually</li> <li>3. No interoperability standard between badge issuers</li> <li>4. No trusted issuer registry to verify badge authority</li> <li>5. Learning Agreement negotiated manually by academic coordinators</li> <li>6. Process takes weeks; outcomes vary by institution pair</li> </ol> | <ol style="list-style-type: none"> <li>1. Student shares EDC transcript from wallet</li> <li>2. Host institution verifies credentials instantly via trust registry</li> <li>3. Structured ELM data maps directly to Learning Agreement fields</li> <li>4. Compatibility with Erasmus Without Paper services</li> <li>5. Pre-recognition of credits agreed before departure based on structured data</li> <li>6. Return recognition automated using same credential infrastructure</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>No common data model across EU institutions. Badge quality varies enormously. No connection to Erasmus Without Paper infrastructure. Administrative burden is high and scales poorly across alliance partners. Trust level: high friction, low scalability.</i></p>                                                                                                                           | <p><b>What EDC enables</b></p> <p><i>EDC integrates directly with EU mobility infrastructure (Europass, Erasmus Without Paper, European Student Card Initiative). Cross-border verification is immediate. Learning Agreement preparation is data-driven. Trust level: low friction, EU-infrastructure aligned.</i></p>                                                                                                                                                                       |

## Key takeaways

- Open Badges have no integration with Erasmus Without Paper or the European Student Card Initiative. EDC is designed for exactly this ecosystem.
- The bottleneck in Erasmus mobility is not travel or housing - it is the Learning Agreement. EDC makes that a structured data exchange. Open Badges keep it a manual negotiation.
- Scalability only comes with standardisation. A university alliance processing hundreds of mobility cases per year cannot do that manually - EDC enables the automation; Open Badges do not.

### Alliance value

A common EDC framework across alliance partners means mobility between them becomes the easiest case, not the hardest.

## Scenario 3 of 7

## A.4 Admissions to Postgraduate Programme

### Context

A graduate applies for a master's programme at a university in another EU country. The admissions team must evaluate prior qualifications, language of instruction, and credit load.

Actors: Applicant · Admissions office · Academic committee · National recognition authority

## Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                                                                                                  | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Applicant submits badge portfolio alongside PDF transcripts</li> <li>2. Admissions team evaluates each badge: issuer reputation, criteria description, evidence links</li> <li>3. No standard for assessment rigour or QA</li> <li>4. No legal identity binding - cannot confirm the applicant is the badge earner</li> <li>5. Badges treated as supplementary at best; decision based on PDF documents</li> </ol> | <ol style="list-style-type: none"> <li>1. Applicant presents EDC from wallet</li> <li>2. Admissions system verifies cryptographic signature and issuer registration</li> <li>3. Structured data read: degree level, EQF, ECTS, language, QA body</li> <li>4. Identity confirmed via eIDAS-linked identifier in credential</li> <li>5. Automated eligibility pre-check against programme requirements</li> <li>6. Committee reviews pre-filtered, verified candidate pool</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>Trust is subjective and issuer-dependent. No legal or identity guarantee. Badges cannot substitute for official documentation in regulated admissions processes. They add noise, not signal. Trust level: supplementary at best, ignored at worst.</i></p>                                                                                                                                                          | <p><b>What EDC enables</b></p> <p><i>Identity is cryptographically bound to credential. Issuer is registered and verifiable. Academic data is structured and comparable. Admissions process is faster, more consistent, and legally defensible. Trust level: trusted input for formal institutional decision.</i></p>                                                                                                                                                               |

## Key takeaways

- The fundamental admissions problem is not information - it is trust. Open Badges provide information. EDC provides verified, identity-bound evidence.
- Legal identity binding in EDC means the credential cannot be shared or claimed by someone other than the earner. Open Badges have no equivalent guarantee.
- For regulated programmes or professions, admissions decisions require a legally defensible evidentiary basis. Open Badges cannot provide that. EDC, with an accredited issuer, can.

### Alliance value

Alliance members can define common admission criteria tied to EDC fields, enabling consistent cross-institution admissions and reducing duplicated evaluation work.

## Scenario 4 of 7

## A.5 Diploma and Degree Issuance and Verification

### Context

A university issues a bachelor's or master's degree. The graduate needs to present this credential to employers, professional bodies, and institutions - potentially for decades.

Actors: Issuing university · Graduate · Employer · Professional registration body · Foreign credential evaluation agency

## Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                                                                                                    | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Badge issued representing degree completion</li> <li>2. Badge hosted on issuer platform or embedded in image</li> <li>3. Graduate shares badge link</li> <li>4. Receiver checks hosted assertion - if server is down, verification fails</li> <li>5. No standard for degree-level data: no official classification, no legal identity</li> <li>6. No revocation mechanism if fraud or error is discovered</li> </ol> | <ol style="list-style-type: none"> <li>1. University issues signed EDC diploma to graduate wallet</li> <li>2. Credential anchored in trust registry with cryptographic proof</li> <li>3. Graduate holds credential independently - verifiable without contacting issuer</li> <li>4. Receiver verifies offline: signature, issuer registration, revocation status</li> <li>5. Structured data: degree classification, EQF level, ECTS, programme title, QA body</li> <li>6. Revocation possible if fraud detected - immediately propagated via StatusList</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>Verification depends on issuer server availability. No revocation standard. No legal identity binding. A degree badge from an unrecognised institution looks identical to one from a highly reputable university. Trust level: visually convincing, institutionally weak.</i></p>                                                                                                                                     | <p><b>What EDC enables</b></p> <p><i>Credential is permanently verifiable, issuer-independent, and revocable. Graduate owns the credential in their wallet. Employer or body can verify in seconds without any university involvement. Valid decades after issuance. Trust level: institutionally authoritative, permanently verifiable.</i></p>                                                                                                                                                                                                                    |

## Key takeaways

- Open Badge verification depends on issuer availability. If the university changes platform, merges, or closes, the badge may become unverifiable. EDC is independently verifiable without the issuer.
- Revocation is a legal and reputational requirement. Open Badges have no standard revocation mechanism. EDC includes it by design, with immediate propagation.
- The value of a degree is not just the information it contains - it is the institutional authority behind it. EDC anchors that authority cryptographically. Open Badges do not.

### Alliance value

Alliance members can issue jointly-recognised diplomas as EDCs with shared issuer registration - creating a credential that carries the authority of the whole alliance, not just one institution.

## Scenario 5 of 7

## A.6 Employer Verification

### Context

A graduate applies for a job. The employer's HR team needs to verify qualifications quickly and reliably, without academic context and often across different countries and systems.

Actors: Graduate / applicant · HR team · Applicant Tracking System (ATS) · Professional body (if regulated role)

### Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Applicant adds badges to professional profile or CV</li> <li>2. HR team may or may not check badge metadata</li> <li>3. No standard integration with ATS systems</li> <li>4. Verification depends on employer recognising the badge issuer</li> <li>5. For regulated roles: badge insufficient, official documents requested separately</li> <li>6. Manual follow-up with university common for senior or regulated positions</li> </ol> | <ol style="list-style-type: none"> <li>1. Graduate presents EDC from wallet via verifier portal or API</li> <li>2. Employer system verifies signature and issuer registration automatically</li> <li>3. Structured data extracted: degree, EQF level, field of study, date, institution</li> <li>4. ATS ingests structured credential data directly - no manual entry</li> <li>5. For regulated roles: EDC provides legally defensible credential evidence</li> <li>6. Cross-border verification works identically - no country-specific process</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>Badge value is platform-dependent and network-dependent. No machine-readable integration with HR systems. Zero value for regulated professions. Trust level: useful for visibility, insufficient for verification.</i></p>                                                                                                                                                                                                                | <p><b>What EDC enables</b></p> <p><i>Employer verification is instant, automated, and legally reliable. No manual follow-up with universities. No fraudulent certificates. ATS integration possible. Works identically across EU countries. Trust level: instant, automated, legally reliable.</i></p>                                                                                                                                                                                                                                                      |

### Key takeaways

- Credential fraud is a real cost for employers and institutions. Open Badge images can be copied or faked. EDC with cryptographic binding cannot be forged.
- The HR bottleneck is not seeing qualifications - it is verifying them. Open Badges speed up visibility. EDC speeds up verification. Only the second one reduces cost and risk.
- ATS integration requires structured, machine-readable data. Open Badge metadata is not standardised enough for reliable ATS ingestion. EDC with ELM is designed for exactly this.

### Alliance value

Graduates from alliance institutions carrying EDC diplomas are verifiable by any EU employer in seconds - a direct competitive advantage in graduate employability.



## A.7 Alliance-Internal Recognition and Skills Portfolio

### Context

Within a European university alliance, a student studies at multiple partner institutions over two years. The alliance wants to recognise the full learning journey and make it portable - both for formal credit accumulation and for skills visibility.

Actors: Student · Multiple alliance partner universities · Alliance coordination office · Employers and institutions outside the alliance

### Journey comparison

| Open Badges                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | European Digital Credentials (EDC)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Each partner issues badges for their own modules</li> <li>2. Student accumulates badges in personal portfolio</li> <li>3. Alliance has no shared data model - badge formats vary by institution</li> <li>4. No automatic aggregation of learning across partners</li> <li>5. Employers and external institutions interpret each badge independently</li> <li>6. Skills visibility is good - but no formal credit accumulation path</li> </ol> | <ol style="list-style-type: none"> <li>1. Alliance defines shared EDC credential profiles (common ELM fields, QA references, EQF alignment)</li> <li>2. Each partner issues EDCs using the shared profile</li> <li>3. Student wallet accumulates verifiable credentials from all partners</li> <li>4. Alliance coordination office can verify and aggregate learning automatically</li> <li>5. Full learning journey presentable as a structured, verifiable portfolio</li> <li>6. External institutions and employers verify any individual credential instantly</li> <li>7. Optional: Open Badges derived from EDCs for social sharing and engagement</li> </ol> |
| <p><b>Where it breaks down</b></p> <p><i>Without a shared data model, badges from five alliance partners are five separate claims with no common framework. Aggregation is visual, not semantic. Formal credit accumulation across institutions is impossible without manual intervention at every step. Trust level: good for engagement and visibility within the alliance community.</i></p>                                                                                         | <p><b>What EDC enables</b></p> <p><i>Shared EDC profiles create a common trust and data layer across all alliance partners. Credits accumulate formally. The full learning journey is portable and verifiable. Open Badges can still be used for engagement - but derived from the authoritative EDC, not issued independently. Trust level: formal credit accumulation + portable verified portfolio.</i></p>                                                                                                                                                                                                                                                     |

### Key takeaways

- Open Badges can make the alliance visible. EDC can make it academically real - a space where learning at any partner institution counts formally at all others.
- The badge-first model produces several separate portfolios that happen to share a logo. The EDC-first model produces one coherent learning record that carries the authority of the whole alliance.
- Skills visibility (the Open Badge strength) is not lost in the EDC model - badges are derived from EDCs for professional profiles, CVs, and engagement. The student gets both. The institution gets one authoritative source of truth.

**Alliance value**

This scenario is the central argument for why a university alliance needs EDC. The alliance's credential infrastructure is either a shared trust framework or it is several separate badge systems with a common website. Only one of those creates genuine academic integration.

Scenario 7 of 7

## Appendix B - Glossary

Quick reference for terms used throughout this guide. For fuller treatment, refer to the relevant section.

| Term               | Definition                                                                                                                                                                                                                                                             |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Digital badge      | A visual digital element representing participation or achievement within a closed system. Carries no structured metadata, is not portable, and implies no verification mechanism. Distinguished from an Open Badge.                                                   |
| Open Badge         | A digital badge conforming to the 1EdTech Open Badges standard (currently v3.0). Carries structured, machine-readable metadata (issuer, recipient, criteria, evidence). Portable across compliant platforms and verifiable by any party.                               |
| Credential         | A formal attestation issued by a trusted authority confirming a qualification, competence, or right. Carries institutional trust and, where relevant, legal weight.                                                                                                    |
| Digital credential | A credential issued, stored, and shared digitally. In its strong form (W3C-VCDM): tamper-evident and cryptographically verifiable without contacting the issuer.                                                                                                       |
| Microcredential    | A type of learning achievement defined by the EU Council Recommendation (2022): a record of learning outcomes following a small volume of learning, assessed against transparent criteria, and shareable digitally. Defined by pedagogical rigour, not size or format. |
| EDC                | European Digital Credential. A digitally signed, ELM-structured, cryptographically verifiable credential. Issued under the Europass/EDCI or DC4EU/EBSI lineage.                                                                                                        |
| ELM                | European Learning Model. The semantic ontology that structures EDC. Defines shared meaning across Member States for fields such as EQF level, ECTS credits, assessment method, and QA reference.                                                                       |
| EDCI               | European Digital Credentials Infrastructure. The Europass/EC-based EDC lineage. Credentials are delivered as JSON-LD files with qualified seals; optionally stored in the Europass repository. Production-ready.                                                       |
| DC4EU              | Digital Credentials for Europe. The eIDAS 2.0 / EBSI / EUDI Wallet EDC lineage. Wallet-native, W3C-VCDM based, citizen-mediated credential presentation. Pilot phase, approaching production.                                                                          |

| Term           | Definition                                                                                                                                                                                                                    |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EBSI           | European Blockchain Services Infrastructure. The trust registry and DID infrastructure underpinning the DC4EU EDC lineage.                                                                                                    |
| eIDAS          | Electronic Identification, Authentication and Trust Services. EU regulation governing electronic identity and trust services. eIDAS 1.0 covers qualified seals (used in EDCI); eIDAS 2.0 introduces QEAA and the EUDI Wallet. |
| EUDI Wallet    | European Digital Identity Wallet. Issued by Member States under eIDAS 2.0. The storage and presentation layer for DC4EU credentials. Wallet-native; enables citizen-mediated credential presentation.                         |
| W3C-VCDM       | W3C Verifiable Credentials Data Model. The technical standard underpinning both EDC (DC4EU lineage) and Open Badges v3.0. Defines the issuer/holder/verifier triangle with cryptographic proof.                               |
| DID            | Decentralised Identifier. A type of identifier that enables verifiable, decentralised digital identity. Required for issuers in the DC4EU/EBSI EDC lineage.                                                                   |
| EQF            | European Qualifications Framework. An 8-level framework for comparing qualifications across Europe. A mandatory semantic field in EDC microcredentials.                                                                       |
| ECTS           | European Credit Transfer and Accumulation System. The credit framework used to express learning volume in EDC. A mandatory field in EDC microcredentials under the EU Council Recommendation.                                 |
| QA reference   | Quality Assurance reference. A mandatory field in EDC microcredentials: a reference to the quality assurance framework (typically an EQAR-registered or national QA agency) that covers the issuing institution.              |
| LE→NP          | Legal Entity to Natural Person data transfer model. The institution issues a credential directly to the student. Both EDCI and DC4EU support this model.                                                                      |
| LE→NP→LE       | Legal Entity to Natural Person to Legal Entity (citizen-mediated) data transfer model. The student holds the credential in a wallet and presents it to a relying party. Primary design target of DC4EU/EBSI/eIDAS 2.0.        |
| EMREX          | European student mobility network for exchanging verified academic records. EDC is the expected format for EMREX integration; Open Badges are not part of this infrastructure.                                                |
| StatusList2021 | A W3C specification for credential status (revocation and suspension) used in the DC4EU lineage. Enables both revocation and suspension of issued credentials.                                                                |

## EUNIS Special Interest Group - Mobility & Digital Credentials

Version 1.0 · June 2026

*This document may be freely reproduced and distributed with attribution to EUNIS SIG Mobility & Digital Credentials.*