

WALLET-BASED MICRO-CREDENTIALS IN IMMERSIVE EDUCATION: EUROPEAN GOVERNANCE FOR PRIVACY-PRESERVING VERIFICATION

Alberto Nico¹, Flavio Manganello², Giannangelo Boccuzzi³,
Giancarlo Masi⁴, Rosa Rondinelli⁵, & Martina Ragusa²

¹*Department of Law, University of Bari (Italy)*

²*Institute for Educational Technology, National Research Council (Italy)*

³*Institute for Educational Technology, National Research Council – University of Bologna (Italy)*

⁴*Institute for Educational Technology, National Research Council – University of Modena
and Reggio Emilia (Italy)*

⁵*Department Department of Earth and Geo-Environmental Sciences, University of Bari (Italy)*

Abstract

As European education increasingly experiments with immersive, metaverse-like environments, the portability of learning outcomes across institutions and platforms becomes a practical requirement. In parallel, European policy developments promote micro-credentials and the wider adoption of machine-verifiable attestations, increasingly conceived as wallet-presented verifiable credentials. This trajectory is reinforced by Regulation (EU) 2024/1183, which establishes the European Digital Identity Framework and provides the legal basis for European Digital Identity Wallets. Within immersive learning contexts—where learners may move across multiple platforms, institutions, and communities—credentialing becomes an infrastructure of trust, but also a potential source of privacy risks, particularly through linkability, metadata leakage, identity persistence, and excessive logging. This paper argues that the central governance challenge is not merely issuing digital credentials for immersive learning, but ensuring that credential ecosystems do not evolve into cross-context tracking infrastructures. To address this challenge, the paper develops a technical-legal governance model for privacy-preserving, interoperable educational credentials in the European context. The model combines a lifecycle-based risk taxonomy, privacy-preserving presentation patterns, and institutional governance levers for procurement and policy. It is then applied to a cross-institution European scenario in which immersive course completion is attested through wallet-presented credentials and verified by external institutions or employers. The paper concludes with a blueprint for privacy-preserving credentialing that supports trustworthy recognition of immersive learning outcomes while safeguarding learner privacy, agency, and fairness.

Keywords: *Verifiable credentials, digital identity wallets, data protection, governance, educational metaverse.*

1. Introduction

Immersive and metaverse-like learning environments are increasingly discussed as part of the evolving digital infrastructure of higher education. Their appeal lies in the possibility of supporting distributed participation, simulation-based learning, persistent collaborative spaces, and more flexible forms of learner mobility across institutional and platform boundaries. In such environments, however, portability of learning outcomes becomes more than an administrative convenience: it becomes a condition for the practical recognition of educational achievement beyond the platform in which learning originally occurred. At the same time, scholarship on micro-credentials in higher education has emphasized their growing relevance as modular, transferable, and complementary forms of recognition within broader lifelong learning ecosystems (Ha et al., 2022).

The European policy context gives this question particular urgency. The Council Recommendation on a European approach to micro-credentials promotes common understanding, recognition, and comparability of micro-credentials across learning and employment settings (Council of the European Union, 2022). In parallel, Regulation (EU) 2024/1183 amended the eIDAS framework to establish the European Digital Identity Framework, including European Digital Identity Wallets (European Parliament and Council of the European Union, 2024). The European digital credential ecosystem, as also reflected in Europass, increasingly presents educational credentials as portable, verifiable, and learner-centred instruments for documenting diplomas, certificates, and micro-credentials (Europass, n.d.).

Against this background, this paper argues that wallet-based micro-credentials in immersive education should not be assessed solely in terms of interoperability and trust. They must also be examined as governance infrastructures that shape how personal data circulate across contexts. The crucial issue is that a credential system designed to facilitate recognition may also create new possibilities for correlation, profiling, and identity persistence across institutions, platforms, and verifiers. The aim of the paper is therefore threefold: to analyse how verifiable credential ecosystems can support recognition of learning in immersive environments; to identify the privacy and governance risks associated with issuance, presentation, verification, revocation, and logging; and to propose an institutionally actionable blueprint for privacy-preserving verification in the emerging European wallet ecosystem.

2. Wallet-based credentials in immersive education

Micro-credentials are especially relevant in immersive education because learning in metaverse-like environments is often modular, platform-mediated, and distributed across multiple actors. A learner may complete a virtual laboratory, participate in an avatar-based simulation, or develop skills in a cross-institution immersive course that does not map neatly onto conventional transcript structures. In such settings, machine-verifiable credentials offer a potentially attractive means of documenting specific learning outcomes in a portable and reusable format. That portability, however, only becomes meaningful if other institutions, employers, or platforms can verify the credential in a trustworthy and interoperable way. This is one reason why wallet-based presentation is becoming increasingly important in the European debate (Council of the European Union, 2022; Europass, n.d.).

From a technical and governance perspective, verifiable credential ecosystems are usually described in terms of issuers, holders, verifiers, wallets, and registries. Recent scholarship on self-sovereign identity and digital wallets emphasizes that these ecosystems promise greater user control, data minimisation, and modular trust relationships, but also depend on organizational choices about standards, privacy-enhancing technologies, and role allocation (Babel et al., 2025). In education, the attraction of wallet-based credentials lies precisely in the possibility of moving from institution-centric records toward learner-mediated presentation. Yet this shift does not automatically guarantee privacy. If wallet interactions generate excessive metadata, if verifiers request more attributes than necessary, or if revocation and logging practices are poorly designed, the learner may become more observable across contexts rather than less (Babel et al., 2025).

For immersive education, the stakes are even higher. Metaverse-like learning environments already generate rich behavioural and contextual data, and credentials derived from those environments may implicitly reflect highly granular forms of participation. As a result, credential portability cannot be understood as a purely functional question. It must also be understood as a question of data protection, governance, and educational fairness. This is precisely the problem identified in the abstract, which frames wallet-mediated credentialing as both an infrastructure of trust and a possible vector of linkability, metadata leakage, and identity persistence.

3. Risks and governance challenges across the credential lifecycle

A useful way to analyse these issues is to examine the credential lifecycle. At the issuance stage, institutions must decide what exactly is being attested, how learning outcomes are described, and what identifiers or metadata are embedded in the credential. Even where the attested achievement is legitimate and useful, over-specification may create privacy risks by revealing more about the learner than is needed for later verification. At the storage stage, the governance question concerns where credentials are kept, what the wallet provider can observe, and whether the technical design preserves holder control. At the presentation and verification stages, the central risks concern over-disclosure, linkability, verifier overreach, and the generation of persistent metadata trails. Revocation and auditability introduce further tensions: institutions may require ways to manage invalid credentials, but revocation mechanisms and verification logs can also create additional observability if they are not carefully designed (Flamini et al., 2024; Ramić et al., 2024).

The literature on selective disclosure is especially important here. Recent reviews describe selective disclosure as a core privacy feature of digital credentials, allowing holders to reveal only the attributes necessary for a given transaction rather than exposing the entire credential (Ramić et al., 2024). Cryptographic research also shows that different selective disclosure mechanisms involve trade-offs concerning unlinkability, standard maturity, performance, and support for more advanced proof structures (Flamini et al., 2024). For educational micro-credentials, this means that privacy-preserving verification cannot remain an abstract aspiration: it must be translated into concrete design choices about attribute minimisation, proof mechanisms, verifier requests, and revocation models (Flamini et al., 2024; Ramić et al., 2024).

There is also a governance issue of role allocation. In educational settings, the issuer may be a university, consortium, or training provider; the holder is the learner; the verifier may be another institution, employer, or platform; and the wallet may be provided within a broader EU digital identity ecosystem. Each actor potentially influences the purposes and means of processing. Consequently, privacy-preserving credentialing requires more than good cryptography. It requires institutional rules on who may request which attributes, how long verification logs may be retained, whether secondary use is permitted, and how learners can contest errors, refusals, or inappropriate verification demands.

4. A technical-legal governance model

This paper proposes a technical-legal governance model for metaverse-ready educational credentials structured around three components.

The first is a lifecycle-based risk taxonomy. This taxonomy maps risks across issuance, storage, presentation, verification, revocation, and logging, while distinguishing the governance roles of issuer, holder, verifier, and wallet provider. The purpose is to make visible where privacy risks are likely to emerge and which actor is in the best position to mitigate them. This element corresponds to the lifecycle-based risk taxonomy explicitly described in the abstract.

The second component consists of privacy-preserving presentation patterns. These patterns are grounded in data minimisation, selective disclosure, and purpose limitation. In practice, this means designing credential requests around necessity rather than convenience: a verifier should request only the minimum claims required for the specific educational or employment purpose at stake. Where possible, credential presentation should reduce the exposure of stable identifiers, limit reusable metadata, and avoid creating correlation points between different transactions. This aligns both with the privacy-oriented rationale behind the EU wallet ecosystem and with the technical literature on selective disclosure in digital credentials (European Parliament and Council of the European Union, 2024; Flamini et al., 2024; Ramić et al., 2024).

The third component consists of institutional governance levers. These include procurement requirements, contractual limitations on secondary use, retention rules for logs and verification records, internal policies on role allocation, and procedural safeguards linked to fairness, accessibility, and contestability. In other words, the privacy quality of a credential ecosystem depends not only on protocol design but also on institutional governance choices. A wallet-based system can only be privacy-preserving in practice if the surrounding educational organisation prevents function creep and over-verification. This institutional dimension is also expressly anticipated in the abstract, which highlights procurement, retention, fairness, accessibility, and contestability as core governance levers.

5. Scenario-based application

To illustrate the model, consider a cross-institution European case in which a learner completes an immersive course delivered in a metaverse-like environment. The course provider issues a micro-credential attesting successful completion and specific learning outcomes. The learner stores the credential in a wallet and later presents it to another university for recognition or to an employer as evidence of competence. In a simple interoperability narrative, this appears to be an ideal use case: portable, machine-verifiable recognition of immersive learning. Yet from a governance perspective, the scenario quickly becomes more complex.

The first question concerns what the credential actually contains. A privacy-preserving design would avoid embedding unnecessary contextual details about the immersive platform, persistent learner identifiers, or excessive course metadata. The second question concerns presentation: must the learner reveal the full credential, or only selected attributes relevant to the decision at hand? The third concerns verification and logging: can the verifier confirm validity without creating a durable transaction history that later enables cross-context correlation? Finally, revocation and auditability must be handled in ways that preserve trust without undermining learner privacy. The scenario therefore stress-tests precisely the tension

identified in the abstract: the challenge is not only to issue credentials, but to prevent the credential ecosystem from becoming a distributed tracking infrastructure.

6. Conclusions

Wallet-based micro-credentials offer a promising route for recognising immersive learning outcomes across institutional and platform boundaries in Europe. They fit well with the European push toward portable, machine-verifiable attestations and with the emerging architecture of EU digital identity wallets (Council of the European Union, 2022; European Parliament and Council of the European Union, 2024; Europass, n.d.). Yet their value depends on more than technical interoperability. Without privacy-preserving presentation, restrained logging, and clear institutional governance, educational credentialing can become a mechanism for cross-context visibility rather than learner empowerment (Babel et al., 2025; Flamini et al., 2024; Ramić et al., 2024).

For this reason, trustworthy credentialing in immersive education should be built around three principles: minimum necessary disclosure, bounded observability, and accountable institutional governance. A European approach that combines verifiable credentials with wallet-based control can support recognition, portability, and trust, but only if it resists the temptation to treat verification as an unlimited data extraction opportunity. The ultimate governance question is therefore not whether immersive learning can be credentialed digitally, but how such credentialing can preserve learner privacy, agency, and fairness while remaining interoperable and credible across contexts.

References

- Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, 35, 28.
- Council of the European Union. (2022). *Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability* (2022/C 243/02). Official Journal of the European Union, C 243, 10–25.
- European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Official Journal of the European Union.
- Europass. (n.d.). *European Digital Credentials for Learning*. Retrieved April 19, 2026.
- Flamini, A., Sciarretta, G., Scuro, M., Sharif, A., Tomasi, A., & Ranise, S. (2024). On cryptographic mechanisms for the selective disclosure of verifiable credentials. *Journal of Information Security and Applications*, 83, 103789.
- Ha, N. T. N., Spittle, M., Watt, A., & Van Dyke, M. (2022). A systematic literature review of micro-credentials in higher education: A non-zero-sum game. *Higher Education Research & Development*. <https://doi.org/10.1080/07294360.2022.2146061>.
- Ramić, Š. B., Cogo, E., Prazina, I., Cogo, E., Turkanović, M., Turčinodžić Mulahasanović, R., & Mrdović, S. (2024). Selective disclosure in digital credentials: A review. *ICT Express*, 10(4), 916–934. <https://doi.org/10.1016/j.icte.2024.05.011>