Bridging Erasmus Without Paper and Self-Sovereign Identity: A Verifiable Credential Issuer for Academic Mobility

João Carreira
University of Leiria and Oeste
Leiria, Portugal
joao.r.carreira@ulo.pt

Lourenço Ferreira
University of Leiria and Oeste
Leiria, Portugal
lourenco.ferreira@ulo.pt

Carlos Machado Antunes
University of Leiria and Oeste
Leiria, Portugal
carlos.machado@ulo.pt

Marisa Maximiano
CIIC, University of Leiria and Oeste
Leiria, Portugal
marisa.maximiano@ulo.pt

Ricardo Gomes
University of Leiria and Oeste
Leiria, Portugal
ricardo.p.gomes@ulo.pt

Vítor Távora
University of Leiria and Oeste
Leiria, Portugal
vitor.tavora@ulo.pt

***Abstract*—Erasmus Without Paper (EWP) exchanges academic mobility records between institutions, but its transcript API only covers institutional transfer and leaves records inside institutional systems. We present a verifiable credential issuer that converts staff-approved EWP Transcripts of Records into signed credentials for student wallets under OpenID for Verifiable Credential Issuance (OID4VCI). For an approved transcript, staff can generate an offer bundle pairing a base OID4VCI profile with a profile oriented toward the European Blockchain Services Infrastructure (EBSI). Sphereon Wallet completed issuance with the base profile, whereas the Portuguese Digital Wallet required adapted metadata, endpoints, and token responses. In both documented runs, redeeming one offer issued one credential and canceled the sibling offer. Public verification still relies on the issuer's database for lookup and selective-disclosure revocation, and EBSI trust-registry accreditation remains future work.**

***Index Terms*—Erasmus Without Paper, academic mobility, verifiable credentials, OID4VCI, EBSI, wallet interoperability**

I. Introduction

The Erasmus Without Paper (EWP) Incoming Mobility Transcript of Records (ToR) API lets sending institutions retrieve transcripts from host institutions in European Learner Mobility Objects (ELMO) XML format [1]. Because this exchange only connects institutional systems, it defines no workflow for issuing a signed copy that a student can hold and present to third parties. Self-sovereign identity addresses this gap through student-held verifiable credentials, while the European Blockchain Services Infrastructure (EBSI) anchors issuer accreditation on a permissioned ledger and keeps academic data off-chain [2].

ELMO to EBSI Diploma Schema (ELMO2EDS) converts Enabling Mobility on Recognition of External studies (EMREX) records into EBSI credentials [3], and Blockcerts defines an open standard for blockchain-anchored credentials [4], yet neither connects to the EWP transcript review process. Our system imports uploaded ELMO XML files matching the EWP ToR schema, and live EWP retrieval remains future work. Staff review and approve each transcript before creating offers, connecting this step to dual-profile issuance, public verification, and two-wallet message comparison.

II. Architecture and Implementation

A. Approval and issuance

The backend validates each uploaded ELMO XML file against the EWP ToR schema, stores the transcript in a database, and displays it in an administrative interface. Once approved, staff can generate two expiring offers, one per wallet profile. The backend stores a SHA-256 hash of each offer's random code for lookup alongside the full link for email resending, and emails links and QR codes to the student for token exchange under OID4VCI [5]. A database lock on the bundle ensures that redeeming one offer issues the credential and invalidates the sibling offer in one transaction.

The base profile issues Selective Disclosure JSON Web Token (SD-JWT) credentials [6], letting holders reveal selected academic fields. The EBSI-oriented profile targets the Portuguese Digital Wallet (PDW), adapting OID4VCI Draft 11 metadata conventions [7] and issuing a W3C Verifiable Credentials Data Model v1.1 payload signed as a JWT-VC [8]. Both profiles sign credentials with ES256 and embed the SHA-256 hash of the imported XML file as source evidence. Both formats carry the student's identifiers, home and host institutions, mobility period, completed courses, grades, and total ECTS credits, which SD-JWT encodes as individually disclosable fields.

Offers follow the OID4VCI pre-authorized code flow [5]: each link carries a random code that is emailed only to the student and becomes unusable on first redemption or when the offer expires, as with standard emailed sign-in links. Possession of the link therefore stands in for student authentication, since integration with institutional identity providers

TABLE I
COMPARISON OF ISSUER PROFILES AND RECORDED WALLET OUTCOMES

Step	Sphereon Wallet (base)	PDW (EBSI-oriented)
Metadata	OID4VCI v1.0 configurations map	Draft 11 credentials list with types
Token	Standard endpoint returning opaque token	Adapted endpoint returning JWT, ID token, and nonce
Credential	SD-JWT with selective disclosure	JWT-VC with Status List 2021 entry
Outcome	1 documented success	1 documented success after adaptations

was outside the scope of this proof of concept. Each credential records the subject decentralized identifier (DID) from the wallet's proof.

B. Verification and trust

A public verification portal accepts a credential string for either profile, checks the issuer signature, expected DID claims, and validity dates, and looks up the SHA-256 hash of the full string in the issuer's database. A validly signed token absent from the database is rejected as unrecognized, whereas recognized credentials load the academic summary from that record. Hashing the full string means removing optional fields from an SD-JWT breaks verification, so selective presentations require matching each disclosed field's hash against the signed digests [6]. Because the portal checks credential strings, it confirms what was issued rather than who presents it; holder binding and replay protection require key-bound presentations.

SD-JWT revocation state is kept only in the issuer's database. EBSI-oriented credentials also reference an index in a published, GZIP-compressed Status List 2021 token that exposes no student data or revocation reasons [9]. Because our implementation orders status bits differently from the specification [9], external status checks remain unconfirmed. The issuer uses `did:web` and keeps transcripts off-chain, leaving EBSI Trusted Issuers Registry accreditation [2] for future work.

C. Interoperability evaluation

Validation combined automated backend tests using 22 XML import samples with seven end-to-end scenarios across the backend, database, email service, administrative interface, and verification portal. The sample set comprises 20 valid transcripts with varied course lists and grading scales, one base reference file, and one malformed file, confirming that unapproved records and expired offers are rejected. Each documented wallet run issued one credential and canceled the competing offer, and the portal accepted the active credential and rejected it after revocation.

Both profiles exchange the pre-authorized code at the token step (Table I). During development, PDW stopped after receiving a valid discovery response from the base profile. Once the issuer exposed Draft 11 metadata and returned a signed JWT access token with an ID token and nonce, PDW requested a JWT-VC with a wallet proof and completed issuance with the adapted response, including a status list reference. Wallet builds, the OID4VCI revision targeted by Sphereon, and total attempt counts were not recorded.

III. CONCLUSION

The two documented runs show that an EWP approval workflow can issue one wallet credential per offer bundle across clients with incompatible protocol expectations. Future work will integrate live EWP retrieval, repeat trials with logged builds and attempt counts, and harden issuance with wallet proof validation, persistent token sessions, and strict bearer checks. Student authentication can start with the transaction code of OID4VCI, sent over a second channel, and move to the institution's identity provider or to identity data presented from a European Digital Identity (EUDI) Wallet, which Member States must offer by the end of 2026. External verification requires SD-JWT disclosure-digest checks, key-bound presentations, public SD-JWT revocation, Status List 2021 bit-order alignment, and EBSI Trusted Issuers Registry accreditation.

ACKNOWLEDGMENT

This work was financially supported by Project BlockchainPT – Decentralize Portugal with Blockchain Agenda, WP 9: Capacitation, 02/C05-i01.01/2022.PC644918095-00000033, funded by the Portuguese Recovery and Resilience Program (PRR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program. João Carreira and Lourenço Ferreira acknowledge University of Leiria and Oeste for the financial support of their scientific research fellowship (BII).

REFERENCES

[1] Erasmus Without Paper Consortium, "Incoming Mobility Transcripts of Records API," v3. [Online]. Available: https://github.com/erasmus-without-paper/ewp-specs-api-imobility-tors/tree/stable-v3 [Accessed: Nov. 2026].

[2] EBSI DevHub, "Trust chains and trusted issuers." [Online]. Available: https://hub.ebsi.eu/docs/services/trust-chains-and-trusted-issuers [Accessed: Nov. 2026].

[3] P. Herbke and H. Yildiz, "ELMO2EDS: Transforming educational credentials into self-sovereign identity paradigm," arXiv:2406.11525, 2024. [Online]. Available: https://arxiv.org/abs/2406.11525

[4] Blockcerts Community, "Blockcerts: The open standard for blockchain credentials." [Online]. Available: https://www.blockcerts.org/ [Accessed: Nov. 2026].

[5] OpenID Foundation, "OpenID for Verifiable Credential Issuance 1.0," final specification, Sep. 2025. [Online]. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-final.html

[6] D. Fett, K. Yasuda, and B. Campbell, "Selective Disclosure for JSON Web Tokens (SD-JWT)," RFC 9901, Nov. 2025, doi:10.17487/RFC9901.

[7] OpenID Foundation, "OpenID for Verifiable Credential Issuance," draft 11, Feb. 2023. [Online]. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-11.html

[8] W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, Mar. 2022. [Online]. Available: https://www.w3.org/TR/vc-data-model-1.1/

[9] W3C, "Verifiable Credentials Status List v2021," First Public Working Draft, Apr. 2023. [Online]. Available: https://www.w3.org/TR/2023/WD-vc-status-list-20230427/