EPiC Series in Computing

Volume 109, 2026, Pages 196–208

Proceedings of EUNIS 2026 Annual Congress

Digital Diplomas in the POL-On System: Centralised Verification and Governance in Polish Higher Education

Michał Doligalski[1], Emil Podwysocki[2] and Marek Michajłowicz[2]

[1] Ministry of Science and Higher Education of Poland

[2] The National Information Processing Institute, Poland

michal.doligalski@mnisw.gov.pl, emil.podwysocki@opi.org.pl, marek.michalowicz@opi.org.pl

Abstract

This article examines the architectural design and implementation of digital diplomas in Poland's higher education sector. Driven by the strategic vision and regulatory framework established by the Polish Ministry of Science and Higher Education (MNiSW), this nationwide digital transformation aims to fundamentally modernise academic credentialing. Developed and maintained by the National Information Processing Institute (OPI PIB) under the direct auspices of the MNiSW, the centralised Electronic Diploma Repository (RDE) operates as a foundational component of the national POL-on system. By evaluating the system's integration, data governance, cryptographic foundations, and cybersecurity protocols, this article highlights how the infrastructure ensures compliance with MNISW policies, maximises security, and enables seamless verification. Ultimately, this MNiSW-spearheaded initiative aims to eliminate credential forgery and to streamline administrative workflows for universities, employers, and graduates, setting a new standard for national public e-services.

1 Introduction and the role of POL-on

In an era of globalisation and increased mobility in the job market, the credibility of traditional, paper-based education credentials is a matter of growing concern. The phenomenon of so-called ‘diploma mills’ and increasingly easy access to advanced techniques for the creation of physical documents pose a serious challenge to academic institutions, employers, and state administrators (Ezell, 2020). The lack

L. Desnos, C. Diaz, J. Mincer-Daszkiewicz, L. Merakos, R. Vogl, S. McLellan and U. Lucke (eds.), EUNIS 2026 (EPiC Series in Computing, vol. 109), pp. 196–208

of fast, universal, and fully reliable mechanisms for verifying traditional diplomas leads to abuse, including the unauthorised provision of specialised services (Lomas, 2021). In response to these critical systemic vulnerabilities, international organisations and researchers point to the urgent need for the systemic digitalisation of educational credentials (UNESCO, 2023). Replacing paper records with cryptographically secured, integrated repositories and digital diplomas is becoming not just an administrative convenience, but a technological necessity. Such an approach enables flawless, real-time verification of qualifications, restoring transparency and absolute trust in higher education systems (Otto et al., 2021).

The modernisation of academic record-keeping has made the secure issuance and verification of university credentials a priority for educational institutions worldwide. This article examines the deployment and ongoing management of digital diplomas in Poland. To fully grasp the scale and significance of this initiative, it must be situated in the broader context of the country's national academic IT infrastructure. As comprehensively detailed by Michajłowicz (2025), the POL-on system serves as the central information system for science and higher education in Poland, functioning as the digital backbone of the whole sector. For over a decade, POL-on has aggregated vast amounts of systemic data—ranging from institutional accreditations and employee records to student lifecycles—to support state financing, public policy, and institutional evaluation.

Driven by the National Information Processing Institute (OPI PIB), the new Electronic Diploma Registry (RDE) leverages this mature, pre-existing infrastructure. Rather than operating as an isolated technological experiment, the RDE is deeply integrated into the POL-on ecosystem, providing a unified, tamper-proof database of higher education qualifications that relies on the established trust and data structures of POL-on (Michajłowicz, 2025).

Establishing this centralised registry required complex technical challenges to be overcome, data from dozens of independent university student information systems (SISs) to be harmonised, and strict national legal frameworks to be followed. A critical success factor in this nationwide deployment has been the implementation of comprehensive data governance at OPI PIB. The governance framework guarantees data integrity, privacy, and interoperability across the country's academic ecosystem. This article outlines the system's architecture, discusses the practical benefits for its stakeholders, and presents conclusions based on the postimplementation analysis of the POL-on digital diploma repository.

While many European countries have developed digital diploma infrastructures – such as Norway’s Vitnemålsportalen (Unit, 2021), Estonia’s blockchain-based initiatives, or Italy’s CIMEA-DiploMe (Pecchioli & Ruffini, 2020) – the Polish approach is unique due to its deep integration with the pre-existing, comprehensive POL-on system. Unlike decentralized models, Poland’s RDE acts as a single source of truth, leveraging a decade of centralized data collection to ensure immediate validity. This design was inspired by the need for a 'once-only' principle, ensuring that no additional data entry is required from universities.

2 The ecosystem and diploma lifecycle

The e-diploma implementation project is a large-scale endeavour that encompasses over 300 entities that are authorised to issue diplomas in the Polish higher education system. It is estimated that the system will process approximately 300,000 diplomas for university graduates and 8,000 documents that confirm academic degrees annually. The transformation schedule assumes a two-stage approach: the option for the voluntary issuance of diplomas in electronic form will begin on 30 June, 2026, while the universal obligation will commence on 1 January, 2027. The effective implementation of this system requires extensive legislative changes, primarily in the Law on Higher Education and Science and the Act on the *mObywatel* application, Poland's national digital wallet application.

The repository requires that specific roles and processes be defined for the issuing institutions. The key roles include:

- Mass import process manager: Typically a nontechnical user whose role is to oversee the data imports executed by a university's IT tools. They have access to a list of asynchronous imports in which they can search by date range and monitor errors (e.g. checking which documents in a batch were rejected)
- Document template administrator: A user who is responsible for adding, removing, and disabling diploma templates and their respective translations
- Communication administrator: A user who manages the security certificates that protect the connection between a university's local systems and the central repository.

The lifecycle of a digital diploma begins with its preparation and registration by a university. The document's content is then verified and officially signed by an authorised person. Following these steps, the document is made available to the user. A graduate (the document owner) can access it through platforms like *mObywatel* to download digital certificates. Simultaneously, external parties—such as university recruitment systems, educational service portals, and HR systems—can instantly verify the authenticity and correctness of a graduate's diplomas directly against the repository.

Digital services for citizens: access and distribution

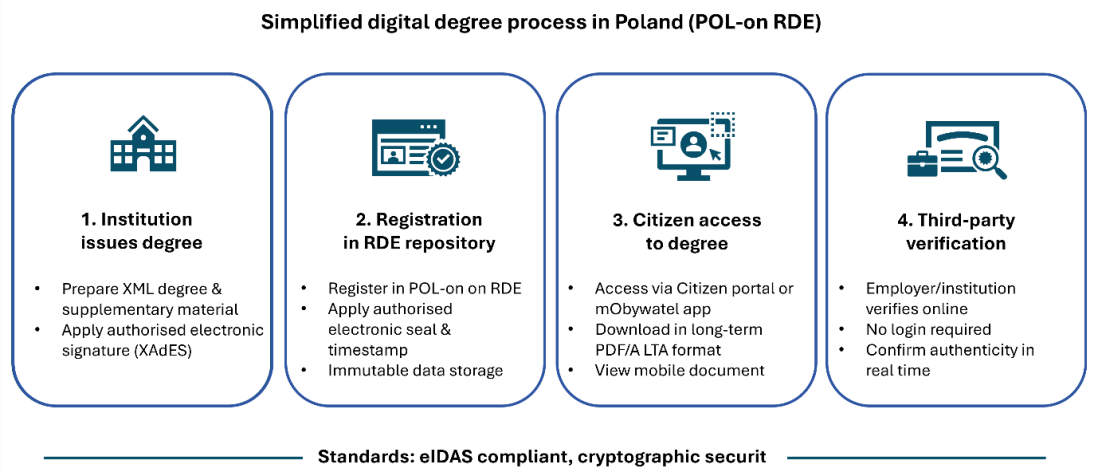

Figure 1. The four-stage lifecycle of a digital diploma within the POL-on ecosystem: illustrating the progression from institutional issuance and cryptographic registration in the RDE, to citizen access via the mObywatel app, and real-time third-party verification.

The implementation of e-diplomas expands the catalog of civic e-services considerably. Graduates gain quick and secure access to their documents via a dedicated citizen portal. The authentication mechanism is based on proven electronic identification nodes (trusted profile, electronic banking, and the *mObywatel* application). For long-term archiving and presentation purposes (e.g. during a recruitment process), a user can download the document in the PDF/A standard (with the long-term archiving profile). Citizens may also view their diplomas in the form of mobile documents in the *mObywatel* application (m-document). The system enforces that a document be transferred to third parties exclusively in electronic form; any, even the slightest, attempt to modify such a file causes a mathematical breakdown of the hash and irreversible damage to the electronic seal, unequivocally exposing forgeries.

3 Diploma verification and summary

The final element of the architecture is a widely accessible verification e-service. It enables employers and institutions to confirm the validity of a diploma online, directly in the RDE resources, using a document's unique identification data (without the need to create an account or log in).

In summary, the realisation of the e-diploma implementation project will result in the launch of sixteen public e-services that cover the full lifecycle of a document: from its issuance, through its sharing, to its verification and possible invalidation. This initiative aligns with the broader trend of digitalisation in public administration, fulfilling the fundamental ‘once-only' principle. Diploma data entered into the RDE can be reused multiple times in other administrative and economic processes, stimulating the digital transformation in Poland further.

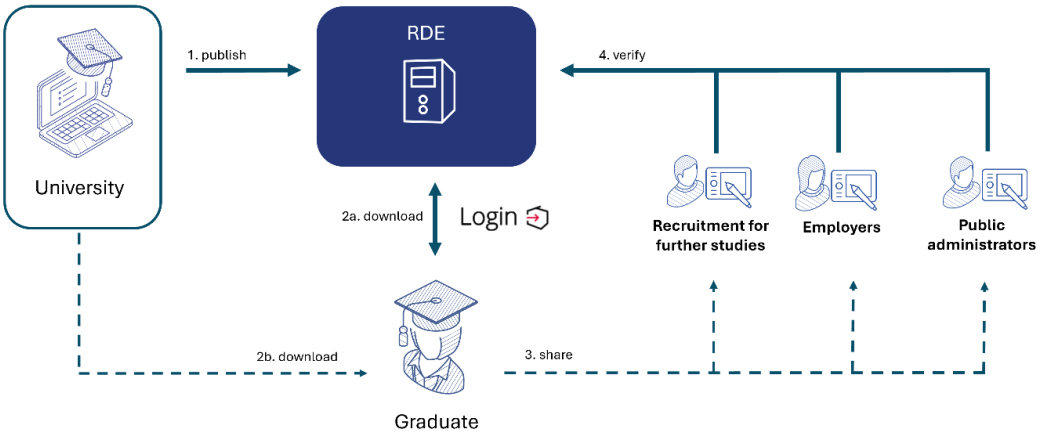

Figure 2. Data flow architecture and stakeholder interactions within the Electronic Diploma Registry (RDE), mapping the credential pathways between higher education institutions, graduates, public administrators, and verifying entities (employers).

Figure 3. The citizen-facing portal of the Electronic Diploma Registry (RDE)

4 System architecture and integration

The heart of the new system is the RDE, which serves as an integrated public registry in the nationwide POL-on system. Its primary role is the secure storage of documents, their long-term preservation, and the ensurance of high data availability and consistency. The RDE will act as the

single source of truth for graduates, employers, and verifying institutions. The database will collect not only first- and second-cycle degree diplomas, but also doctoral and postdoctoral diplomas and supplements, as well as digital transcripts and decisions on document invalidation.

From a technical standpoint, an e-diploma is a structured digital document created in XML format. The generation process requires interaction from a university (the issuing institution), which prepares the data package. This document is then signed using a qualified electronic signature in the XAdES standard by a university's rector or another authorised person. Before final registration in the system, the RDE conducts rigorous validation, checking the completeness of the XML structure, the substantive correctness of the data, and the validity of the cryptographic certificates used for the signatures. Successful registration concludes with the file being stamped with the repository's authorised electronic seal and an authorised time stamp, permanently blocking any possibility of its modification. Under the new legal regime, the traditional paper diploma has lost its status as the primary information carrier; it has become secondary to the electronic diploma and is issued only at the request of a graduate.

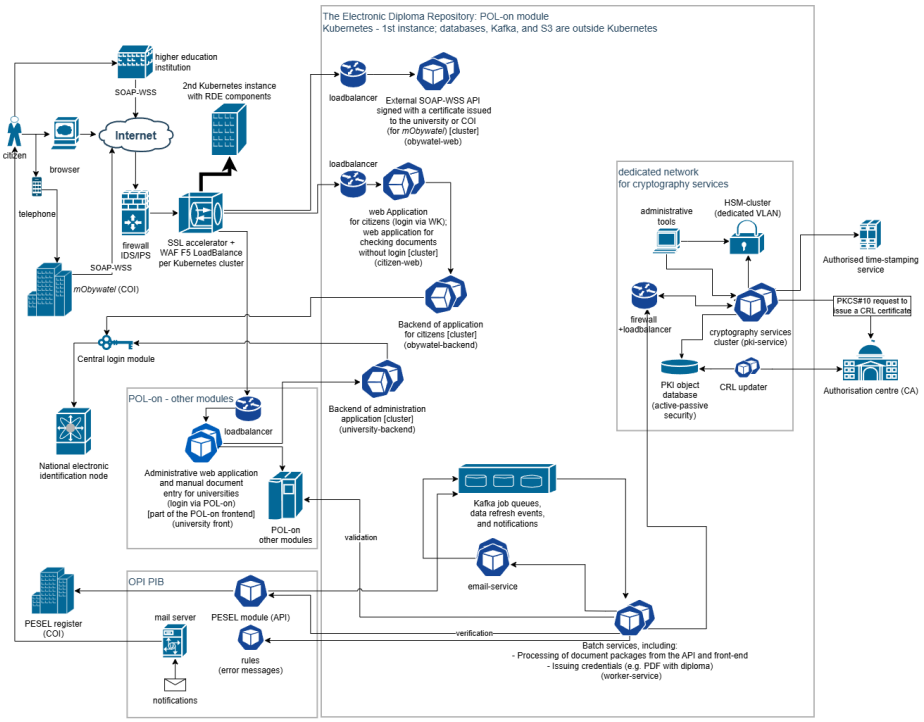

Figure 4. Architectural diagram of RDE

Figure 4 illustrates the interaction between the University's Student Information Systems (SIS), the central RDE repository, and external verification nodes. The complexity reflects the multi-layered security required for state-level data. The architecture employs standardized XML schemas for diploma templates, ensuring machine-readability and semantic interoperability across national registries, which aligns with the European Learning Model (ELM) standards. Figure depicts the logical flow of data between internal OPI modules and external API consumers. The 'Verification Node' acts as a gateway,

ensuring that only validly structured requests (compliant with national XML schemas) reach the RDE core.

5 System cooperation and interoperability

A registry of this scale cannot operate in isolation. The success of the RDE relies on its complex integration with various external state and institutional registries.

The system cooperation model dictates direct and indirect data flows between the following nodes:

- Local university systems: Academic institutions utilise secure APIs to transmit diploma data directly from their internal SISs to the central POL-on repository
- PESEL registry: Integration with the national identification (PESEL) database ensures the precise verification of graduates' identities
- *mObywatel e*cosystem: The repository interfaces directly with the *mObywatel* system . When a diploma is registered and signed in POL-on, the relevant data is pushed via APIs (compliant with IT entre guidelines) to the user's mobile application, enabling citizens to carry and present their credentials digitally
- Central login module (SSO): Access to administrative interfaces is secured via a centralised single-sign-on module, which ensures that only authenticated institutional personnel can perform sensitive operations
- External verification portals: Enterprise systems, university recruitment portals, and dedicated services for higher education can programmatically query the RDE to verify the authenticity of a candidate's credentials.Cybersecurity of event logging in the ecosystem of digital diplomas and the POL-on system

The increasing digitalisation of academic processes—including the issuance, storage, and verification of digital diplomas— has elevated the importance of cybersecurity in higher education governance. In Poland, the POL-on system serves as the central register for academic degrees and qualifications, integrating data from all higher education institutions and providing authoritative verification mechanisms. As these digital infrastructures process highly sensitive personal and institutional data, maintaining their integrity demands robust mechanisms of accountability, transparency, and security.

A foundational component of this security landscape is the management of event logs, which record system, user, and application activities across the ecosystem. Event logs play a dual role: they are essential for detecting anomalies and cyber threats, and they serve as formal evidence that supports regulatory compliance and institutional accountability. The cybersecurity requirements that govern event logging in digital diploma infrastructures such as POL-on are shaped by a comprehensive regulatory and standards framework that integrates European data protection law, national interoperability guidelines, and internationally recognised information security norms. At the core of this framework lies the General Data Protection Regulation (GDPR), which establishes accountability, integrity, and transparency as foundational principles that govern the processing of personal data. The

GDPR further mandates that all activities that involve such data, including those captured in system logs, must be demonstrably traceable and justifiable. Complementing GDPR, the Polish National Interoperability Framework (KRI) mandates minimum organisational and technical safeguards for public information systems, including precise requirements for log retention, time synchronisation, and access control, thereby ensuring uniform cybersecurity baselines across the institutions that participate in national registries. Moreover, international standards such as ISO/IEC 27001 and ISO/IEC 27002 provide systematic guidelines for implementing secure logging practices, defining controls that relate to monitoring, incident detection, and the protection of evidential data. Additional technical guidance from frameworks such as NIST SP 800-53 and the OWASP Secure Logging recommendations further strengthen operational resilience by addressing emerging threats, cryptographic integrity protections, and risks associated with credential leakage or log tampering. Together, these legal and normative sources create a multilayered governance environment that ensures that event logging processes in the digital diploma ecosystem are not only secure, but also auditable, interoperable, and aligned with global best practices—all of which are essential for maintaining trust in higher-education credentialing.

Event logging forms a core security and governance mechanism in digital diploma ecosystems, ensuring that the accuracy, integrity, and legal validity of academic records can be verified through the complete traceability of system behaviour. In national-scale infrastructures such as POL-on, logs provide authoritative evidence of authentication events, configuration changes, and all interactions with protected resources, supporting both incident investigation and regulatory compliance. To fulfil this role, each log entry must contain a coherent and granular set of attributes —including unique user or service identifiers, network source metadata, synchronised timestamps, geolocation when available, and precise descriptions of executed operations and their outcomes— while explicitly excluding sensitive secrets such as passwords, tokens, or API keys to prevent the logs themselves from becoming a vector of compromise. Ensuring the evidential value and reliability of logs further requires strict access control, with all administrative interactions recorded in a dedicated audit trail, as well as tamper-resistant storage mechanisms such as WORM repositories, cryptographically chained entries, digital signatures, and automated integrity verification processes in centralised aggregation systems. Because chronological consistency is essential for correlating events across distributed components, all systems that contribute to the logging infrastructure must synchronise with trusted, redundant NTP sources. Finally, the operational continuity and long-term trustworthiness of logs depend on continuous monitoring, automated anomaly detection, systematic review by authorised personnel, resilient backup strategies, and adherence to statutory retention periods—which typically require the secure preservation of logs for a minimum of two years before their permanent sanitisation. Together, these principles establish a secure, verifiable, and audit-ready logging environment that underpins the resilience, transparency, and forensic readiness of digital credentialing systems.

To mitigate the risk of uncontrolled data correlation, the RDE verification portal does not offer a search function. Verification is strictly transactional: the verifier must already possess the document's hash or unique ID provided by the holder. Furthermore, rate-limiting and anomaly detection are implemented at the infrastructure level to prevent automated 'scraping' of diploma data, ensuring that the system cannot be used for mass data harvesting.

6 Cryptographic Foundations and Document Integrity

The integrity and non-repudiation of digital diplomas in the RDE system are guaranteed by a multi-layered cryptographic process. Rather than relying on a single validation point, the system employs a "dual-signature" workflow that ensures both the provenance of the document from the university and its secure storage in the national repository.

6.1 The Signing Workflow

The process of issuing a digital diploma follows a strictly defined sequence to ensure legal validity under the eIDAS framework:

- University-Level Signature: The process begins at the Higher Education Institution (HEI). An authorized representative of the university (e.g., the Rector or a designated Dean) signs the diploma data using a qualified electronic signature. This signature, typically in the XAdES format, encapsulates the graduate's data and the degree details, providing proof of the document's origin.
- Centralised Repository Sealing: Once the signed document is transmitted to the POL-on system, the RDE infrastructure applies a second layer of protection—a qualified electronic seal. This seal is issued by the National Information Processing Institute (OPI) and acts as a corporate signature of the repository itself.
- Long-Term Validation (LTA): To ensure that the diploma remains verifiable for decades, even after the original signing certificates expire, the system applies a Long-Term Data with Archive Timestamp (LTA) profile. This involves adding qualified timestamps to the signature, which proves that the document existed in its current form at a specific point in time and that the certificates were valid when the signature was applied.

6.2. Role of the Hardware Security Module (HSM)

To ensure the secure handling of critical cryptographic operations, the RDE relies on a centralized Hardware Security Module (HSM). Its responsibilities are strictly defined to guarantee the highest level of protection for private keys and digital seals:

- Secure Key Storage – The HSM securely stores the private keys used to generate OPI electronic seals. It does *not* store private keys belonging to university rectors—those remain under the control of individual HEIs or qualified trust service providers.
- Centralized Governance and Integrity Protection – By using an HSM to apply the final repository seal, the Ministry of Science and Higher Education ensures that once a diploma is ingested into the RDE, its state becomes immutable. The document is protected by certified, state-grade hardware, preventing any unauthorized alteration by internal or external actors.
- Verification Without Authentication – Each sealed document is represented by a unique cryptographic hash. This hash allows third parties—such as employers—to verify the authenticity of a diploma through the RDE’s public verification node, without needing to

authenticate or access the POL-on system. This approach preserves both accessibility and data integrity.

When a university publishes a diploma to the RDE, the system sends the final, canonical representation of the document to the HSM via a secure, authenticated channel. Inside the HSM, the private sealing key is used to compute a digital signature over the diploma's hash. The signed hash is returned to the RDE, where it becomes the "repository seal". Crucially, the private key never leaves the hardware module, and the RDE cannot perform the signing operation on its own – ensuring that only the Ministry-controlled HSM can produce valid repository seals. As a result, even if an attacker gained administrative access to the RDE infrastructure, they would still be unable to forge or alter a sealed diploma.

7 eIDAS2 in the context of the DC4EU initiative

The evolution of Europe's digital identity landscape under the revised eIDAS Regulation (eIDAS2) profoundly shapes the objectives and architecture of the Digital Credentials for Europe (DC4EU) initiative, which pilots largescale implementations of verifiable educational and social security credentials across the European Union. eIDAS2 introduces the European Digital Identity Wallet (EUDI Wallet) as a unified mechanism through which residents can store and present verifiable attributes, credentials, and identity data with full cross-border legal validity. This enables a shift from traditional centralised verification models towards decentralised, user-centric trust architectures. This regulatory framework establishes binding interoperability, cryptographic integrity requirements, and trust service standards that apply directly to the piloted DC4EU use cases in education and social security, including digital diplomas, learning credentials, and health insurance attestations. As highlighted in DC4EU's analysis of the forthcoming transition, the alignment with eIDAS2 represents a structural transformation of the European Digital Credentials for Learning (EDCL) ecosystem—from classical public-key-infrastructure–based verification to a hybrid model that combines PKI, decentralised identifiers (DIDs), and electronic attestations of attributes (EAAs), which provides enhanced cross-border portability, privacy, and user sovereignty over data sharing. Under eIDAS2, all European Union member states must deploy an officially certified EUDI Wallet, which enables credentials issued in DC4EU pilots (such as diplomas or social security A1 certificates) to be stored locally by users and verified instantly without contacting the issuer, through cryptographic proofs embedded in the credential itself. The RDE is designed to be future-proof. Integration with the eIDAS2 framework and the European Digital Identity Wallet (EUDI) is currently being tested within the DC4EU project. This will allow Polish graduates to present their credentials across borders seamlessly, using the PESEL registry for national identification and eIDAS-compliant nodes for cross-border student mobility.

Consequently, the Polish digital credentialing framework has been preliminarily tested and verified within this pan-European context, driven by the active participation of the National Information Processing Institute and several Polish universities in the DC4EU pilots.

8 Conclusions

The implementation of the Electronic Diploma Repository (RDE) within the POL-on system represents a monumental shift in the digitalization of Poland's higher education sector. Driven by the Ministry of Science and Higher Education (MNISW) and developed by the National Information Processing Institute (OPI PIB), this nationwide infrastructure successfully addresses the vulnerabilities of traditional paper credentials, such as the growing threat of 'diploma mills' and credential forgery. By transitioning to a unified, tamper-proof database, the system enables flawless, real-time verification of academic qualifications, thereby restoring transparency and absolute trust for universities, employers, and graduates.

A critical factor in the success of this large-scale deployment is the rigorous application of comprehensive data governance, cybersecurity, and cryptographic standards. The integration of hardware security modules (HSMs) guarantee that every digital diploma is protected by qualified electronic seals and timestamps. Furthermore, compliance with robust frameworks like the GDPR, the Polish National Interoperability Framework (KRI), and ISO/IEC 27001 establishes a highly secure, auditable event-logging environment that is essential for maintaining institutional accountability and defending against cyber threats.

Ultimately, this initiative transcends national modernization by aligning with the broader European digital identity landscape. Through compatibility with the revised eIDAS Regulation (eIDAS2) and the DC4EU initiative, the Polish digital diploma ecosystem is prepared for seamless cross-border interoperability via the European Digital Identity Wallet (EUDI Wallet). By fulfilling the fundamental 'once-only' principle of public administration, the RDE not only streamlines administrative workflows but also operationalizes a user-centric, pan-European credentialing infrastructure where individuals exercise full sovereign control over their educational attestations.

9 References/Citations

Bylina, M., Podwysocki, E., & Michajłowicz, M. (2023). Data Governance at the National Information Processing Institute in Poland. Paper presented at the EPiC Series in Computing, 95, 7988. https://doi.org/10.29007/1rp9.

Michajłowicz, M. (Ed.). (2025). Information technology systems that support science and higher education: POL-on: A central information system for science and higher education in Poland. National Information Processing Institute. https://opi.org.pl/en/what-we-do/science-and-research/science-for-everyone/publishing-house/

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*.

Fisher, J., & Leder, G. (2023). Micro-credentials and reflections on higher education. *Higher Education Evaluation and Development, 17*(2), 96-112. https://doi.org/10.1108/HEED-01-2023-0004

Ezell, A. (2020). Detecting fake university degrees in a digital world. In E. Denisova-Schmidt (Ed.), *Corruption in higher education: Global challenges and responses* (pp. 112-117). Brill.

Lomas, T. (2021). Blockchain and higher education diplomas. *PubMed Central (PMC)*.

Otto, D., et al. (2021). Digital credentials in higher education institutions: A literature review. *ResearchGate*.

UNESCO. (2023). *Transforming the digital landscape of higher education in Latin America and the Caribbean*.

Pecchioli, S., & Ruffini, G. (2020). Digital Credentials and Blockchain: The CIMEA-DiploMe Ecosystem for the Recognition of Qualifications. In Proceedings of the EUNIS 2020 Congress.

Unit – Directorate for ICT and Joint Services in Higher Education and Research. (2021). The Diploma Registry: Sharing Results from Higher Education in Norway.

10 Author biographies

Michał Doligalski (PhD) is the Head of the Department of Innovation and Development Ministry of Science and Higher Education of Poland

Michał Doligalski, He obtained his PhD in 2011 from the Faculty of Computer Science, Electrical Engineering, and Automation at the University of Zielona Góra, specializing in embedded systems. H His scientific interests include embedded systems, the Internet of Things (IoT), satellite navigation systems, and multidisciplinary research in computer science and biomedical engineering. He has contributed numerous publications in the field of Computer science and biomedical engineering. His projects and research interests focus on applied research in collaboration with industry. Currently, he focuses on systemic solutions in legislation and the design and implementation of digitalization solutions for higher education and scientific institutions.

Email: michal.doligalski@mnisw.gov.pl

LinkedIn: https://www.linkedin.com/in/michaldoligalski/

People of Science: https://ludzie.nauka.gov.pl/ln/profiles/micha%C5%82.doligalski.CtM7CfMI6Iq

Emil Podwysocki (MSc) is the Deputy Head of the National Information Processing Institute (OPI PIB) in Poland.

He has more than a decade of professional experience and is a certified expert in enterprise architecture, business intelligence systems, low-code software development, and IT service management based on ITIL best practices. His areas of interest include data management, cybersecurity, DevOps practices, and the practical application of low-code technologies to streamline and automate business processes. He graduated from the Lodz University of Technology with a master's degree in telecommunication systems. He also completed an MBA programme for IT professionals at the Polish–Japanese Academy of Information Technology.

Email: emil.podwysocki@opi.org.pl

LinkedIn: www.linkedin.com/in/emil-podwysocki

People of Science: https://ludzie.nauka.gov.pl/ln/profiles/emil.podwysocki.Uhm5e5gJnem

Marek Michajłowicz (MSc) is the Deputy Head of the National Information Processing Institute (OPI PIB) in Poland.

He has over a dozen years of professional experience in designing and developing large-scale IT systems that support science and higher education. Throughout his career, he has been instrumental in the implementation of key nationwide projects, including the Integrated System of Information on Science and Higher Education (POL-on), the Uniform Anti-plagiarism System (JSA), and the grant management system (OSF). He holds a degree in IT Engineering and is a graduate of the MBA program at the Warsaw University of Technology Business School, as well as the Business Informatics program at the Warsaw School of Economics (SGH)

Email: marek.michajlowicz@opi.org.pl

LinkedIn: https://www.linkedin.com/in/marek-michajlowicz/

People of Science: https://ludzie.nauka.gov.pl/ln/profiles/marek.michaj%C5%82owicz.W8ZeBuzoc6I