EPiC Series in Computing

Volume 107, 2025, Pages 314–323

Proceedings of EUNIS 2025 annual congress in Belfast

Development of a Demonstrator for Issuing Electronic Learning Certificates for the EU Digital Identity Wallet

Marlies Gollnick[1], Alexander Jacobs[1], Robin Kopitz[1],
Meiko Lips[1], and Patrick Rempel[1]

Harz University of Applied Sciences, Wernigerode, Germany
mgollnick@hs-harz.de, ajacobs@hs-harz.de, rkopitz@hs-harz.de,
mlips@hs-harz.de, prempel@hs-harz.de

Abstract

The revised eIDAS 2.0 Regulation of 2024 creates the framework for the future European Union Digital Identity Wallet. This is intended to create a uniform digital identity for EU citizens from 2026. The paper analyzes the key components of this new technical architecture and presents a feasibility study to issue electronic learning certificates for the European Union Digital Identity Wallet.

1 Introduction

With the entry into force of Regulation (EU) Nr. 910/2014 on electronic identification and trust services for electronic eIDAS Regulation internal market (eIDAS Regulation) [35], trust services could be offered in all 28 EU member states. The eIDAS Regulation replaced the Signature Directive [34] and introduced electronic seals as a new service. A central element is electronic identification (eID), which focuses on the interoperability of identification systems in the European single market in order to make cross-border administrative services more efficient.

As a result, many Member States have implemented corresponding eID systems, e.g. Germany with the online ID function of the ID card [7]. Nevertheless, technologies and security standards vary between member states. Since 2016, digital habits and the range of online services have developed considerably. An evaluation by the European Commission [12] also showed that the implementation of the regulation fell short of expectations. Too few member states were using eID systems and cross-border interoperability was only partially achieved. In particular, organizational interoperability problems were hindering practical use. The report also criticizes the inadequate consideration of sector-specific requirements by the eIDAS Regulation. However, there is agreement on the relevance of the regulation and its objectives. In response, the European Union (EU) adopted Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0) [38] to create a European framework for a digital identity. The eIDAS 2.0 obliges the member states to provide EU citizens with a digital identity in the form of a European Union Digital Identity Wallet (EUDI Wallet). This creates uniform conditions for the cross-border use of national electronic means of identification and electronic attribute certificates.

L. Desnos, R. Vogl, L. Merakos, C. Diaz, J. Mincer-Daszkiewicz and S. Mclellan (eds.), EUNIS 2025 (EPiC Series in Computing, vol. 107), pp. 314–323

2 European Union Digital Identity Wallet

The eIDAS 2.0 regulation formulates specifications and objectives for the introduction of a trustworthy, voluntary and user-controlled digital identity [38], which is to be implemented within the EU. These goals are to be realized by the European Union Digital Identity Wallet (EUDI Wallet) [13]. According to Article 5(4)(a) eIDAS 2.0, the EUDI Wallet enables users to digitally authenticate themselves as both natural and legal persons and to manage electronic attribute certificates, including their request, storage and presentation [38]. Control over the transfer of data lies entirely with the users and is intended to ensure the highest level of security and data protection [38]. The EUDI Wallet is currently being tested in four large pilot projects with eleven use cases: Potential for European Digital Identity [29], EU Digital Wallet Consortium (EWC) [10], Nordic-Baltic eID (NOBID) [26], and Digital Credentials For Europe (DC4EU) [11].

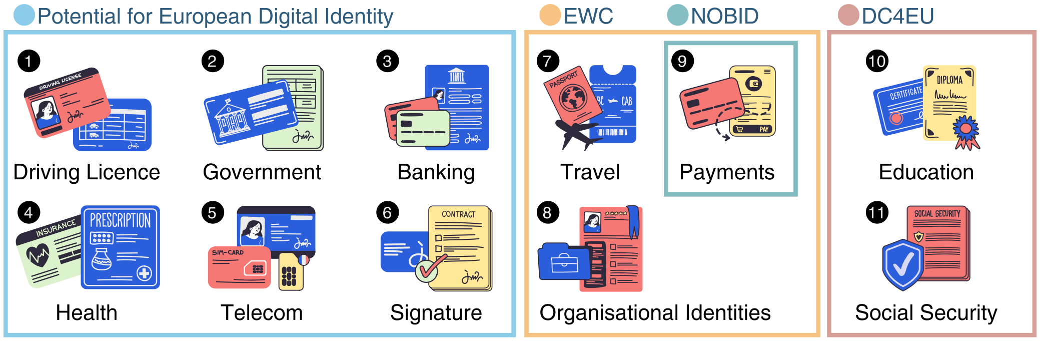


Figure 1: EUDI wallet use cases and distribution to pilot projects, based on [9]

Figure 1 shows the use cases and their distribution across the pilot projects [9]: ❶ digital driver's license, ❷ access to public services (national borders and EU-wide) through secure login, ❸ identity verification when opening an account, ❹ picking up prescriptions, ❺ identification for SIM card applications, ❻ creation of digital signatures, ❼ storage of travel documents, ❽ proof of company or organizational affiliation, ❾ authentication and payment authorization, ❿ digital proof of education and ⓫ Digital social security card.

For these use cases, Person Identification Data (PID), Qualified Electronic Attestation of Attributes (QEAA), and Electronic Attestation of Attributes (EAA) are implemented in the EUDI Wallet [38]. According to Article 3(a) of eIDAS 2.0, PIDs are used to establish the identity and authentication of natural or legal persons and their representatives [38]. Article 3(j) defines EAA as an electronic certificate that enables the authentication of attributes. It also defines that QEAAs must be issued by qualified trust service providers [38]. The difference between QEAA and EAA is of a legal nature. The technical representation of the attributes is similar [33].

Specific regulations for the implementation of eIDAS 2.0 are made in the form of implementing acts. The first were adopted on 28th November 2024 and published in the European Official Journal on 4th December 2024 [37]. Among other things, they define the core functions and integrity of the EUDI Wallet. They also regulate their certification, the verification of the authenticity and validity of wallet units, the identification of EUDI Wallet providers and the issuing of PIDs and EAAs. In addition, regulations for protocols and interfaces, the identity of registered relying parties and the presentation of PID and EAA attributes to relying parties and other wallet entities are regulated.

3 Architecture of the EUDI Wallet

In addition to the legal requirements of eIDAS 2.0 and the implementing acts, the Architecture and Reference Framework (ARF) [37] provides a technical specification of the EUDI Wallet architecture.

The ARF was created on the basis of Recommendation (EU) 2021/946 of the European Commission [36]. The implementation of the demonstrator in this feasibility study is based on version 1.4.1 of the ARF published on 11th November 2024 [37].

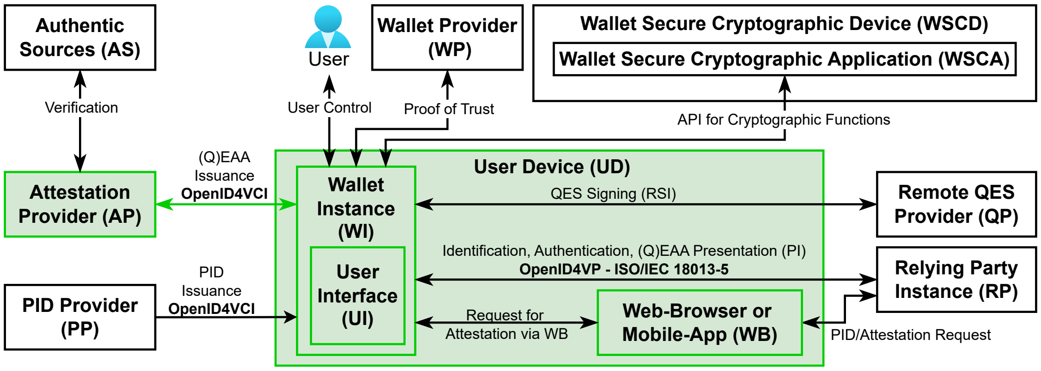

Authentic Sources (AS)
Verification
User
User Control
Wallet Provider (WP)
Proof of Trust
Wallet Secure Cryptographic Device (WSCD)
Wallet Secure Cryptographic Application (WSCA)
API for Cryptographic Functions
Attestation Provider (AP)
(Q)EAA Issuance
OpenID4VCI
User Device (UD)
Wallet Instance (WI)
QES Signing (RSI)
Remote QES Provider (QP)
User Interface (UI)
Identification, Authentication, (Q)EAA Presentation (PI)
OpenID4VP - ISO/IEC 18013-5
Relying Party Instance (RP)
PID Issuance
OpenID4VCI
PID Provider (PP)
Request for Attestation via WB
Web-Browser or Mobile-App (WB)
PID/Attestation Request

Figure 2: Components of the EUDI Wallet demonstrator in the context of the ARF

Figure 2 shows the main components of the ARF reference architecture for the EUDI Wallet. The components implemented in the demonstrator for issuing electronic learning certificates are marked in green. The individual components are described in more detail below.

- The *User Device (UD)* represents the device on which the Wallet Instance (WI) operates.
- The *Wallet Instance (WI)* represents an application installed on the UD, which is assigned to the user and is controlled by the user via the *User Interface (UI)*. In addition to the WI, a *Web-Browser or Mobil-App (WB)* can be executed on the same or another UD.
- The *Wallet Secure Cryptographic Device (WSCD)* combines trusted hardware and firmware to provide both a secure storage for cryptographic values and a protected environment for the execution of cryptographic applications such as the *Wallet Secure Cryptographic Application (WSCA)*.
- The *Wallet Provider (WP)* supports the WIen, carries out maintenance work and performs wallet instance attestations via the Wallet-Provider-Interface (WPI).
- The *Attestation Provider (AP)* is responsible for issuing certificates and uses the *Authentic Sources (AS)* for this purpose.
- The *PID Provider (PP)* is responsible for issuing PID.

- The *Remote QES Provider (QP)* is used for the remote signature with Qualified Electronic Signatures (QES).
- The *Relying Party Instance (RP)* acts as an acceptance and verification instance for PIDs or (Q)EAAs from the wallet.

The components communicate with each other via corresponding interfaces and protocols. The protocols used here are the OpenID for Verifiable Presentation-Protocol (OpenId4VP) [27] and the OpenID for Verifiable Credential Issuance-Protocol (OpenID4VCI) [32] in accordance with the ISO/IEC 18013-5 standard [16].

The OpenID4VCI protocol [32] is used for issuing (Q)EAAs. This distinguishes between *Authorization Code Flow* (authorization during the (Q)EAA issuance process) and *Pre-Authorized Code Flow* (authorization before the (Q)EAA issuance process). For further consideration, a *Pre-Authorized Code Flow* flow for (Q)EAA issuance as depicted in Figure 3 is assumed.

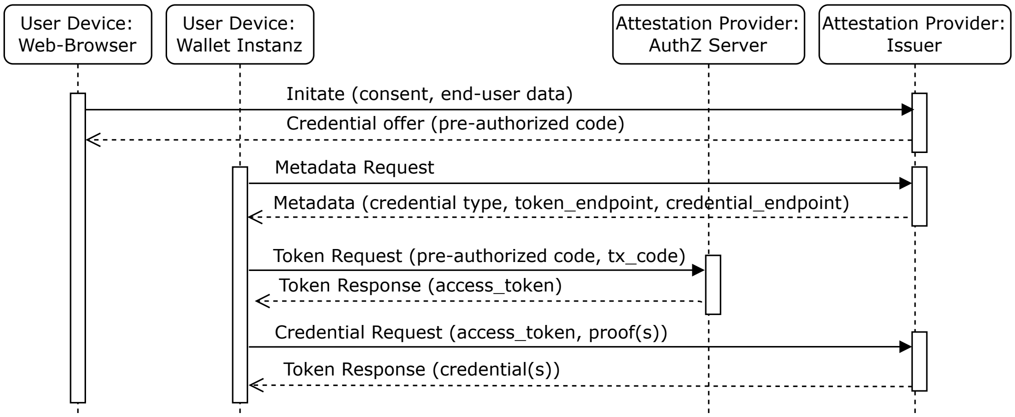

User Device: Web-Browser
User Device: Wallet Instanz
Attestation Provider: AuthZ Server
Attestation Provider: Issuer
Initate (consent, end-user data)
Credential offer (pre-authorized code)
Metadata Request
Metadata (credential type, token_endpoint, credential_endpoint)
Token Request (pre-authorized code, tx_code)
Token Response (access_token)
Credential Request (access_token, proof(s))
Token Response (credential(s))

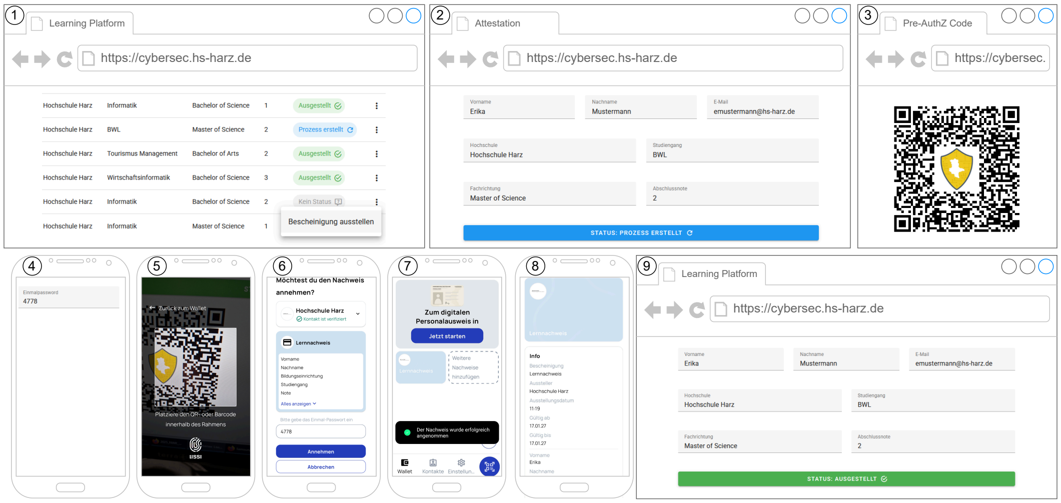
Figure 3: Credential issuance flow

The user requests a (Q)EAA from the attestation provider via an application (WB). After a time delay, the user receives a message that the requested (Q)EAA is available. With the wallet instance, the user establishes a connection to the attestation provider and receives information on the metadata of the (Q)EAA from the provider. By entering a code, the user proves the previously issued authorization. The wallet instance now requests the attestation provider to transmit the (Q)EAA data and then receives it so that the (Q)EAA can be stored in the wallet instance.

4 Feasibility of Issuing Electronic Learning Certificates

This feasibility study focuses on the issuing of electronic learning certificates as an example of QEAAs in the EUDI Wallet. Lecturers certify the attributes (e.g. topic, final grade) of the learning certificates. These learning records are to be made available to course participants in electronic form for their EUDI Wallet.

To this end, we developed a web-based learning platform to issue certificates using the following technology stack: PostgreSQL for storing the learning platform data, C# back-end



① Learning Platform — https://cybersec.hs-harz.de

Hochschule Harz	Informatik	Bachelor of Science	1	Ausgestellt	⋮
Hochschule Harz	BWL	Master of Science	2	Prozess erstellt	⋮
Hochschule Harz	Tourismus Management	Bachelor of Arts	2	Ausgestellt	⋮
Hochschule Harz	Wirtschaftsinformatik	Bachelor of Science	3	Ausgestellt	⋮
Hochschule Harz	Informatik	Bachelor of Science	2	Kein Status	⋮
Hochschule Harz	Informatik	Master of Science	1		

Bescheinigung ausstellen

② Attestation — https://cybersec.hs-harz.de

Vorname: Erika
Nachname: Mustermann
E-Mail: emustermann@hs-harz.de
Hochschule: Hochschule Harz
Studiengang: BWL
Fachrichtung: Master of Science
Abschlussnote: 2

STATUS: PROZESS ERSTELLT

③ Pre-AuthZ Code — https://cybersec.

④ Einmalpassword: 4778

⑤ ← Zurück zum Wallet

Platziere den QR- oder Barcode innerhalb des Rahmens

LISSI

⑥ Möchtest du den Nachweis annehmen?

Hochschule Harz
Kontakt ist verifiziert

Lernnachweis
Vorname
Nachname
Bildungseinrichtung
Studiengang
Note
Alles anzeigen

Bitte gebe das Einmal-Passwort ein: 4778

Annehmen
Abbrechen

⑦ Zum digitalen Personalausweis in
Jetzt starten

Lernnachweis
Weitere Nachweise hinzufügen

Der Nachweis wurde erfolgreich angenommen

⑧ Lernnachweis

Info
Bescheinigung: Lernnachweis
Aussteller: Hochschule Harz
Ausstellungsdatum: 11:19
Gültig ab: 17.01.27
Gültig bis: 17.01.27
Vorname: Erika
Nachname

⑨ Learning Platform — https://cybersec.hs-harz.de

Vorname: Erika
Nachname: Mustermann
E-Mail: emustermann@hs-harz.de
Hochschule: Hochschule Harz
Studiengang: BWL
Fachrichtung: Master of Science
Abschlussnote: 2

STATUS: AUSGESTELLT

Figure 4: Feasibility study - issuing electronic learning certificates for the EUDI Wallet

for process control, Typescript and Vue for the user interface. For communication between the attestation provider and the wallet instance, we implemented *Pre-Authorized Code Flow* in accordance with the OpenID4VCI protocol. Therefore we leveraged the Lissi EUDI Wallet Connector [22]. In addition, we used the most recent beta version of the Lissi EUDI Wallet [23] to verify and validate our demonstrator. As depicted in Figure 4, the process of issuing electronic learning certificates for the EUDI Wallet comprises the following steps.

① First, the role*Lecturer* opens the learning platform in the web browser and selects *Issue certificate*.

② This confirms the participation in the course and initiates *Pre-Authorized Code Flow* to issue the proof through the back-end.

③ A *Credential Offer* is created, and the status of the issue changes to *Process created*. The role *Participant* receives this *Credential Offer* in the form of a QR code.

④ The role *Participant* scans the QR code and initiates the issuance of the electronic learning certificate in the EUDI Wallet.

⑤ Optionally, the role *Participant* receives the corresponding one-time password (OTP) via a different channel.

⑥ Once the OTP is entered, an access token is generated to initiate the attestation process. The wallet can then use this token to retrieve the corresponding attestation data from our learning platform, which serves as the attestation provider.

⑦ The message "Attestation has been successfully accepted".

⑧ The role *Participant* can be seen in the EUDI Wallet under "Learning certificates".

⑨ The status of the issuance on the learning platform changes to "successful issued".

5 Related Work

The EUDI Wallet ecosystem is currently experiencing very dynamic developments. Both its legal and technical foundations are undergoing continuous adjustments and changes. For instance, the eIDAS 2.0 regulation refers to forthcoming implementing acts, which will define more detailed provisions [14]. At the same time, the technical architecture and reference framework (ARF) is being regularly updated and expanded. The rapid evolution of the ARF is evident from the frequency of new releases: version 1.4.1 was published on 05.09.2024, followed by version 1.5.0 on 04.02.2025, version 1.6.0 on 03.03.2025, version 1.7.0 on 17.03.2025, and version 1.8.0 on 27.03.2025 [1]. Biedermann et al. [3] present a systematic literature review (SLR) on the topic of "knowledge of technological developments that led up to implementation of eIDAS 2.0 covering relevant publications from 2005 to 2024". In a related study, Bertram et al. [2] explore technologies for deniable authentication in signature-based credential-systems. The authors examine three key approaches in detail: deniable zero-knowledge, time-based deniability, and designated verifiers. Lepore et al. [20] investigate the interoperability between eIDAS 2.0 and existing frameworks, with a particular focus on mapping eIDAS 2.0 entities to the Trust Over IP framework. To support this mapping, the authors employ a graph alignment method, which also enables a clear visual representation of the relationships. With the growing adoption of decentralized identity management solutions, [30] analyzes the EUDI Wallet as a representative implementation. The study examines its application in the banking, eHealth, and digital credentials sectors. In addition, the authors review key challenges and threats related to privacy and the design of the eIDAS 2.0 framework. Using the MUSAP libraries, Bukhari et al. [8] propose a unified signature API for Secure Signature Creation Devices (SSCDs) that complies with eIDAS 2.0. Their approach enables developers to request multiple Levels of Assurance (LoA) signatures regardless of the programming language, SSCD platform, or underlying technology (centralized or decentralized) [8]. Blasco et al. [4] provide an overview of the current state of eIDAS 2.0 and the EUDI Wallet, highlighting conceptual similarities to the Digital Euro. Morales et al. [24] introduce the ACME High (ACMEH) protocol, which replaces HTTP with HTTPS. According to the authors, this design introduces a trade-off between enhanced security and verification flexibility versus increased communication overhead compared to the standard ACME protocol. Sel et al. [31] focus on approaches to measuring trustworthiness and develop a local graph database based on data from the eIDAS 2.0 Trust List to support this analysis. Zafeiropoulou [40] maps the attributes of Digital Identification Documents within the European Union, with a particular emphasis on the EUDI Wallet. The study highlights that "the ISA^2 Core Vocabularies and OpenID Connect are not overlapping" [40], underlining potential challenges in achieving semantic and technical interoperability. Lampropoulos et al. [19] examine DIMANDS2, a framework designed to organize identity data and enable secure, privacy-preserving exchanges of identity information between service providers and identity issuers—while giving users full control over their identity data. Given its decentralized nature, the framework presents a promising candidate for potential implementation within the EUDI Wallet. Lindquist [21] examines various privacy standards in the context of digital identification and digital wallet technologies. The author references the eIDAS 2.0 regulation for digital identification and the EUDI Wallet as a standard for wallet implementations. Bochnia et al. [5] propose the concept of Long-Lived Verifiable Credentials (LLVCs) for use cases such as educational diplomas. The authors discuss the key requirements and challenges associated with LLVCs and outline potential strategies to address these challenges. The security and privacy of wearable technologies in relation to the EUDI Wallet are examined in [28]. In this context, multi Trusted Execution Environments (TEEs) are proposed—described as "a distributed TEE architecture for heterogeneous device clusters, enabling secure data exchange and cooperation between TEEs". In [18], blind signatures and their potential risks to security and privacy are studied. As a countermeasure, a transparent watchdog is proposed, and its effectiveness is demonstrated through empirical proof. Wich et al. [39] focus on the implementation of QES using Selective Disclosure JSON Web Tokens (SD-JWT) in combination with OpenId4VP. In [6], general requirements for SSI software in organizational structures are identified, and existing gaps in current SSI solutions are highlighted. In [25], an approach is presented to improve the trustworthiness of Service Providers (SPs) in digital wallet systems. For this purpose, an open-source authorized Accreditation Body (AB) is utilized, which can be integrated into the EUDI Wallet. Inza discusses in [17] the current state of the EUDI Wallet in the context of the eIDAS Regulation and its amendment under eIDAS 2.0 and provide a list of related standards relevant to the EUDI Wallet. The implementation of EMREX in the large-scale pilot project Digital Credentials for Europe (DC4EU) is discussed in [15]. EMREX is used for system-to-system communication in the educational sector and is described as contributing to greater interoperability within this domain.

6 Summary and Future Work

The new eIDAS 2.0 regulation creates the framework for the future EUDI Wallet. This will create a uniform digital identity for EU citizens from 2026. This article analyzes the key components of this new architecture and presents a feasibility study for issuing electronic proof of identity. This demonstrates the functionalities of a qualified AP. The new regulation is currently still in progress, as can be seen from the publication of the first implementing regulations [37] and the planned publication of the reference standards for EUDI Wallets [14]. As part of the further development of the reference standards, the EUDI wallet demonstrator is to be continuously improved as part of the *CyberSecurity-Verbund LSA II Identity, Access and Trust Management* project at the Harz University of Applied Sciences and its feasibility, security and user-friendliness validated with further studies.

7 Acknowledgments

We are funded by the program "Sachsen-Anhalt WISSENSCHAFT Forschung und Innovation (EFRE)": ZS/2023/12/182029. We would like to thank Lissi [23] for their extensive technical support and for providing the wallet beta version [22] for the Android and iOS platforms.

References

[1] European Digital Identity Wallet - Architecture and Reference Framework - Version 1.8.0, 2025.

[2] Magdalena Bertram, Maximilian Richter, and Marian Margraf. Achieving Third-party Deniability in Signature-based Credential Systems. In *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 2327–2333, July 2024.

[3] Ben Biedermann, Matthew Scerri, Victoria Kozlova, and Joshua Ellul. A Systematisation of Knowledge: Connecting European Digital Identities with Web3. In *2024 IEEE International Conference on Blockchain (Blockchain)*, pages 605–610, August 2024.

[4] Ainhoa Inza Blasco. Digital Identity in a European User-Centric Ecosystem and Its Similarities with the Digital Euro Proposal. In Carmen Pastor Sempere, editor, *Governance and Control of*

Data and Digital Economy in the European Single Market, volume 71, pages 453–471. Springer Nature Switzerland, Cham, 2025.

[5] Ricardo Bochnia and Jürgen Anke. Long-Lived Verifiable Credentials: Ensuring Durability Beyond the Issuer's Lifetime. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pages 1–9, Vienna Austria, July 2024. ACM.

[6] Ricardo Bochnia, Daniel Richter, and Jürgen Anke. Self-Sovereign Identity for Organizations: Requirements for Enterprise Software. *IEEE Access*, 12:7637–7660, 2024.

[7] BSI. German eID - Overview of the German eID system. Technical Report Version 1.4, BSI, 2020.

[8] Ammar Bukhari, Jarmo Miettinen, and Muttukrishnan Rajarajan. Defining Unified Signature API Library for Mobile Apps to Integrate with Secure Signature Creation Devices (SSCDs). In *2024 IEEE International Conference on Blockchain (Blockchain)*, pages 619–624, Copenhagen, Denmark, August 2024. IEEE.

[9] European Commission. The many use cases of the EU Digital Identity Wallets. [online]. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet [Accessed 7. Jan. 2025].

[10] EU Digital Identity Wallet Consortium. Introducing The EU Digital Identity Wallet Consortium. [online]. https://eudiwalletconsortium.org [Accessed 7. Jan. 2025].

[11] Digital Credentials for Europe. Digital Credentials for Europe. [online]. https://www.dc4eu.eu/ [Accessed 7. Jan. 2025].

[12] European Commission, VVA, Deloitte, and Spark. Evaluation study of the Regulation no.910/2014 (eIDAS Regulation): Final report. Technical report, Publications Office, LU, 2021.

[13] Federal Ministry of the Interior and Community. Sichere digitale Identitäten: Bürgerinnen und Bürger sollen sich mit dem Smartphone ausweisen können. [online]. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/09/eudi-wallet-sep.html?nn=9390260 [Accessed 7. Jan. 2025], September 2024.

[14] Federal Ministry of the Interior and Community. eIDAS 2.0 und EUDI-Wallets. [online]. https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/ [Accessed 8. Jan. 2025], February 2025.

[15] Tor Fridell, Geir Vangen, Janina Mincer-Daszkiewicz, Jan Joost Norder, Kimmo Rautio, Igor Drvodelić, and Guido Bacharach. The future is in your wallet – how EMREX plans interaction with the EUDI wallet. In *Proceedings of European University Information Systems Congress 2023*, pages 209–201, 2023.

[16] International Organization for Standardization. Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application (ISO/IEC 18013-5:2021(en)), September 2021.

[17] Julián Inza. The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation. In Carmen Pastor Sempere, editor, *Governance and Control of Data and Digital Economy in the European Single Market*, volume 71, pages 433–452. Springer Nature Switzerland, Cham, 2025.

[18] Mirosław Kutyłowski and Oliwer Sobolewski. Privacy Illusion: Subliminal Channels in Schnorr-like Blind-Signature Schemes. *Applied Sciences*, 15(5):2864, March 2025.

[19] Konstantinos Lampropoulos, Nikos Kyriakoulis, Giorgos Georgakakos, and Spyros Denazis. Identity Management through a global Discovery System based on Decentralized Identities. In *2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 176–181, November 2023.

[20] Cristian Lepore, Romain Laborde, and Jessica Eynard. Aligning eIDAS and Trust Over IP: A Mapping Approach. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pages 1–9, Vienna Austria, July 2024. ACM.

[21] Jan Lindquist. Introducing Privacy Receipts into DLT and eIDAS. *Journal of ICT*, 2023.

[22] Lissi. Lissi EUDI-Wallet Connector. [online]. https://www.lissi.id/eudi-wallet-connector [Accessed 8. Jan. 2025].

[23] Lissi. Test first use Cases with our EUDI-Wallet Solution. [online]. https://www.lissi.id/for-users [Accessed 9. Jan. 2025].

[24] David A. Cordova Morales, Ahmad Samer Wazan, David W. Chadwick, Romain Laborde, and April Rains Reyes Maramara. Enhancing the ACME protocol to automate the management of all X.509 web certificates (Extended version). *Computer Communications*, 236:108106, April 2025.

[25] Stefan More, Jakob Heher, Edona Fasllija, and Maximilian Mathie. Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pages 1–11, Vienna Austria, July 2024. ACM.

[26] NOBID Consortium. The NOBID Project, 2025.

[27] O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker. OpenID for Verifiable Presentations. [online]. https://openid.net/specs/openid-4-verifiable-presentations-1_0-16.html [Accessed 24. Feb. 2025].

[28] Simon Ott, Benjamin Orthen, Alexander Weidinger, Julian Horsch, Vijayanand Nayani, and Jan-Erik Ekberg. MultiTEE: Distributing Trusted Execution Environments. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 1617–1629, Singapore Singapore, July 2024. ACM.

[29] Potential. Building the Future of Digital Identity in Europe. [online]. https://www.digital-identity-wallet.eu/ [Accessed 7. Jan. 2025], 2023.

[30] Panagiotis Rizomiliotis and Maristel Hairetaki. Decentralized Identity Management and the European Identity Reform. In Nikolaos Pitropakis and Sokratis Katsikas, editors, *Security and Privacy in Smart Environments*, volume 14800, pages 240–255. Springer Nature Switzerland, Cham, 2025.

[31] Marc Sel, Hasin Ishraq Reefat, Naghmeh Karimi, and Konstantinos Mersinas. Evaluation of Entity Trustworthiness Based on Public and Private Data. In Tim Muller, Carmen Fernandez-Gago, Davide Ceolin, Ehud Gudes, and Nurit Gal-Oz, editors, *Trust Management XIV*, volume 694, pages 136–145. Springer Nature Switzerland, Cham, 2024.

[32] T. Lodderstedt, K. Yasuda, and T. Looker. OpenID for Verifiable Credential Issuance - draft 15. [online]. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html [Accessed 24. Feb. 2025], December 2024.

[33] European Union. European Digital Identity Wallet Architecture and Reference Framework, Version 1.4.1 [online]. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/ [Accessed 9. Jan. 2025].

[34] European Union. Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronical signatures, January 2000.

[35] European Union. Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repeating Directive 1999/93/EC, August 2014.

[36] European Union. Commission Recommendation (EU) 2021/946 of June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, June 2021.

[37] European Union. Official Journal L series daily view. [online]. https://eur-lex.europa.eu/oj/daily-view/L-series/default.html [Accessed 24. Feb. 2025], December 2024.

[38] European Union. Regulation (EU) 2024/1183 of the European Parliament and the Council of 11 April 2024 amending Regulaiton (EU) No 910/2014 as regards establishing the European Digital Identity Framework, April 2024.

[39] Tobias Wich, Detlef Hühnlein, Florian Otto, and Mike Prechtl. Qualified Electronic Signatures with the EU Digital Identity Wallet. 2024.

[40] Anna Zafeiropoulou and Evangelos Sakkopoulos. Harmonising Digital Identity Documents. In *2023 14th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pages 1–8, Volos, Greece, July 2023. IEEE.

Biographies of Authors

Marlies Gollnick is a research associate in the research project ”CyberSecurity-Verbund Land Sachsen-Anhalt II - Identity, Access and Trust Management/Infrastructure” that is funded by Saxony-Anhalt and European Union (https://cybersec.hs-harz.de) and works in the Automation & Computer Sciences Department at Harz University of Applied Sciences.

Alexander Jacobs is a research assistant in the research project ”CyberSecurity-Verbund Land Sachsen-Anhalt II - Identity, Access and Trust Management/Infrastructure” that is funded by Saxony-Anhalt and European Union (https://cybersec.hs-harz.de) and works in the Automation & Computer Sciences Department at Harz University of Applied Sciences. He studied Industrial Engineering (B.Eng.) and Technology and Innovation Management (M.Eng.) at Harz University of Applied Sciences.

Robin Kopitz is a developer in the research project ”CyberSecurity-Verbund Land Sachsen-Anhalt II - Identity, Access and Trust Management/Infrastructure” that is funded by Saxony-Anhalt and European Union (https://cybersec.hs-harz.de) and works in the Automation & Computer Sciences Department at Harz University of Applied Sciences. He studied Computer Science (B.Sc. at Harz University of Applied Sciences.

Meiko Lips is a engineer in the research project ”CyberSecurity-Verbund Land Sachsen-Anhalt II - Identity, Access and Trust Management/Infrastructure” that is funded by Saxony-Anhalt and European Union (https://cybersec.hs-harz.de) and works in the Automation & Computer Sciences Department at Harz University of Applied Sciences.

Prof. Dr.-Ing. Patrick Rempel is a Professor for Information Security in Automation & Computer Sciences Department at Harz University of Applied Sciences (https://hs-harz.de/prempel). He leads the research project ”CyberSecurity-Verbund Land Sachsen-Anhalt II - Identity, Access and Trust Management/Infrastructure” that is funded by Saxony-Anhalt and European Union (https://cybersec.hs-harz.de). He is coordinator of the B. Sc. course ”Administrative Digitization and Informatics” at Harz University of Applied Sciences (https://www.hs-harz.de/verwaltungsdigitalisierung).