SecureSystemsDesignandTechnologyDevelopment. VelikoTarnovo, Bulgaria
ProceedingsoftheInternationalScientific Conference,2026. Volume I, 241-245

Assessment of EU Digital Identity Wallet from Security Perspective

Alexander Yankov
Law and History Faculty, South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
alexander.yankov1990@gmail.com
ORCID: 0009-0001-2795-0562

***Abstract* — The European Union tries to introduce a sovereign digital ecosystem centered on the European Digital Identity Wallet (EUDI), a user-controlled instrument designed to combine strong technical safeguards—multi-factor authentication, zero-knowledge encryption, and secure hardware elements (SE/TEE)—with the legal mechanisms such as qualified electronic signatures (QES) under eIDAS 2.0. The wallet promises GDPR-compliant local storage of personal identification data and streamlined access to cross-border digital services, while supporting a risk-based hierarchy of Levels of Assurance (LoA) to match authentication strength to transaction sensitivity. However, the architecture and policy choices that enable these benefits also introduce significant security, privacy and socio-economic risks: key compromise and supply-chain vulnerabilities; tensions between device-centric and cloud-assisted models; potential loss of financial privacy with a digital euro; profiling and exclusion of vulnerable populations; and data minimization. Successful deployment therefore requires not only robust cryptography and certified hardware, but also resilient recovery mechanisms, interoperable standards, transparent governance, independent audits and inclusion policies that balance security, convenience and civil liberties.**

Keywords* — *European Digital Identity Wallet, sovereign digital ecosystem, level of assurance, GDPR, digital euro.

I. Introduction

One of the new aspects of the European Union (EU) development is its efforts to shape a new digital reality based on sovereignty, security and trust. In her 2025 State of the Union address, European Commission President Ursula von der Leyen [1] presented a vision of a future in which digital sovereignty, resilience, data protection and digital identity come to the fore. These principles reflect a reality in which security, privacy and accountability would become not just regulatory requirements but competitive advantages.

The proposal for a European Digital Identity Wallet (EUDI) [2] aims to ensure security through strong multi-factor authentication (MFA) [3], zero-disclosure encryption and secure hardware elements (SE/TEE) [4] in devices. The digital wallet is expected to meet General Data Protection Regulation (GDPR) standards [5], protecting personal data from fraud and giving users control over what information they share. The wallet will allow for the safe storage of personal documents, driving licenses and bank cards, ensuring secure access to digital services across the European Union [6]. At the same time, however, architectural and regulatory solutions create new attack possibilities and institutional risks that require in-depth analysis.

II. Methodology

The study adopts a qualitative, interpretive methodology that triangulates legal-text analysis, standards appraisal, and socio-technical risk assessment to interrogate the design and implications of the European Digital Identity Wallet. It systematically analyzes primary regulatory instruments and technical standards—most notably eIDAS 2.0, GDPR, and ISO 18013-5—treating these texts as both normative frameworks and sources of technical requirements. Complementing this close reading, the paper employs comparative evaluation to contrast device-centric and account-centric architectures (drawing on examples from commercial native wallets) and uses a risk-based analytic lens to map potential threats across technical, institutional, and social dimensions—privacy loss, exclusion, and supply-chain vulnerabilities are foregrounded. Methodological attention is also given to normative implications: the work links technical assurance levels (LoA) to legal and economic outcomes, assessing how different assurance thresholds affect accessibility and trust. In conclusion, the paper situates its findings within broader policy debates, noting that the introduction of a European Digital Identity Wallet is a serious step towards digital integration and legal digitalization in the EU.

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.39

III. EUDI AND THE EUROPEAN SOVEREIGN DIGITAL ECOSYSTEM

Undoubtedly, the European Union is striving to invest in its own technologies, reduce dependence on external suppliers and strengthen control over cloud, hardware and information systems. Digital sovereignty is becoming not only a condition for security, but also a strategic priority on the path to long-term independence. Developing domestic capacities in areas such as cloud technologies, hardware solutions and digital infrastructure would allow Europe to innovate and function without external dependencies [7].

The European Digital Identity Wallet, currently under development, will radically change the way citizens store and share personal information [8]. Legal entities also will need to adapt to the new system, strengthening data protection and strengthening consumer trust. The General Data Protection Regulation is becoming increasingly stringent, not allowing organizations to limit themselves to formal compliance. At its core, the GDPR protects citizens' rights and maintains their trust. Encryption, least privilege access and transparent accountability reduce risks and demonstrate responsible data management.
Europe's digital future depends on whether and to what extent systems and organizations can prove themselves worthy on a daily basis. But it is built on trust [9]. Companies that implement zero trust principles, protect data at all stages and build processes that are aligned with digital sovereignty will not only meet regulatory requirements – they will gain a real competitive advantage in the future. The result will be reliable digital identity protection, regulatory compliance and confidence in the EU's evolving digital requirements.

It should be noted that the EUDI wallet is a fully European solution, with its core infrastructure and identification services meeting the highest European data protection and security standards. It will offer legal entities strategic assurance that sensitive contract and customer data remains in the EU and is not exposed to access from third countries [9].

IV. DISCUSSION ABOUT THE LEVEL OF ASSURANCE AND THE DIGITAL IDENTITY

As is well known, in the digital world, identity is not a binary concept of 'known/unknown', but a spectrum of assurance. The Level of Assurance (LoA) [10] quantifies this assurance, representing the degree of conviction that the person claiming a given identity is indeed its true owner. This is the foundation of digital trust behind every secure transaction and interaction. A higher LoA means a more stringent verification and authentication process, which reduces the risk of fraud, unauthorized access and abuse. Therefore, choosing the right LoA is a critical risk management exercise that must balance security, convenience and accessibility. Therefore, for low-risk actions — such as creating a forum account or changing your address — a lower LoA is acceptable, but for high-risk transactions — accessing financial or medical data, large money transfers, signing contracts — a high LoA is required [11].

The conclusion is that LoA is not an abstract technical rating; it is the 'gateway' that defines what a user can do in the digital world. The LoA, assigned to a digital certificate or required by a service, defines the scope of transactions, the level of access, and the legal force of actions [12].

This is why the trust system and the required LoA are not only a technical but also an economic and social tool. Too high requirements can create a 'digital fortress' inaccessible to a part of the population, limiting digital inclusion. Too low standards lead to fraud, undermine trust in the digital economy and lead to so called 'digital death' [13] of the persons. This tension determines the different approaches of the world's leading economies. A system supporting multiple LoA allows for a flexible architecture tailored to risk. A certificate with a 'high' LoA can be used for services requiring a 'substantial' or a 'low' LoA, but not vice versa. This hierarchy ensures that the level of trust corresponds to the risk.

In this sense, the European Digital Identity Wallet (EUDI) is a central element of the eIDAS 2.0 Regulation [2]. It is designed as a secure, user-controlled application, provided by each Member State, that allows the storage and transmission of personal identification data (PID) [14] and electronic attributes (EAA) [15] – such as a driving license, diploma or prescription.

The abovementioned Regulation requires each Member State to provide its citizens with at least one wallet. The core architectural component is the Wallet Unit, which resides on the user's personal mobile device and relies on a local or remote Wallet Secure Cryptographic Device (WSCD) [16] for its security. This design inherently ties the wallet's highest security features to the context of a specific device. Although the ARF [17] clearly describes the flows for use across devices—for example, using a smartphone to scan a QR code to authenticate a session on a laptop—this is a model of interaction, not synchronization. True synchronization of wallet state, including its private keys and credentials, across multiple devices is technically complex and creates significant security challenges that could conflict with the eIDAS principle of 'single control' by the user [10].

A critical question in wallet architecture is whether digital credentials are tied to the user's device or to their account or the tension between device-centric security and account-centric user experience. ISO 18013-5 [18] is fundamentally device-centric in its security architecture. Its primary goal is to prevent credential cloning and ensure that credential presentation occurs from the authentic device to which the credential was issued. This is achieved through strong device affinity, in which the credential's private keys are stored in a secure, tamper-resistant hardware component of the mobile device, such as a Secure Element (SE) or Trusted Execution Environment (TEE). During presentation, the device performs a cryptographic operation with this key, proving that it is the authentic holder of the credential. The standard explicitly requires that credentials be stored either on the original mobile device or on a server

managed by the issuing authority, reinforcing this device-centric model.

However, the standard does not explicitly prohibit the use of a user account as a management and orchestration layer. This has led to the emergence of a hybrid model, particularly in the native wallet implementations of the companies such as Apple and Google. In this model, the cryptographic security anchor remains the physical device, but a user-facing cloud account (such as an Apple ID or Google Account) serves as the lifecycle management anchor. This account layer can facilitate user-friendly features, such as the migration of credentials to a new, trusted device nearby (in the case of Apple).

A key architectural question would be how the wallet would work across multiple devices. The current architecture (ARF) assumes that the EUDI would not be a typical cloud service with synchronization. Instead, the user would have one primary device — their 'source of trust'. The basic principle in this case would be to have one primary wallet, issued by the Member State and linked to the primary device. However, this would immediately raise the question of how to proceed in cases of dual citizens of two EU Member States and whether they would be allowed to have two independent wallets.

This approach would make EUDI not a 'cloud wallet' but a kind of 'identity hub'. The primary device is required for critical operations. This highlights the need for reliable backup and recovery mechanisms, as losing the device could temporarily block the digital identity.

V. Qualified electronic signature and cryptographic verification

While the authentication process confirms the identity of the wallet holder, the digital signature certifies legal intent. The highest form in the EU is the qualified electronic signature (QES) [19]. According to eIDAS, it has the same legal force as a handwritten signature. A document signed with a QES cannot be rejected just because it is electronic, making QES the 'gold standard' for transactions.

It should be borne in mind that it is likely that the next development within the EU will be multi-wallet. Organizations should support standards such as OpenID4VP [20] and ISO 18013-5 to accept attributes from different wallets — EUDI, embedded wallets of operating systems, and others. At the same time, however, users and holders of e-wallets should be educated to trust cryptography, not the screen. Ordinary people should understand that visual verification of the screen is easy to forge and cryptographic verification is necessary.

VI. EUDI and the digital euro

Last but not least, it should be noted that the claims related to the EUDI and the introduction of the digital euro. The introduction of the EUDI and the digital euro carries some significant risks, such as the loss of financial privacy. While the cash is anonymous, the digital euro could allow for the tracking of absolutely all transactions. Another very likely risk would be the profiling of citizens, as detailed profiles of purchases, habits and location could be used for advertising or control [21]. Not without importance is the exclusion of vulnerable groups – such as people without smartphones, the elderly or people with low digital literacy, who could be excluded from the opportunity to benefit from the European digital wallet.

Next, the role of commercial banks as a kind of guarantor in a number of socio-economic processes will be undermined. They will also lose their place as an intermediary between the central banks of the member states and ordinary citizens and legal entities. When more payments go through the digital euro, banks would certainly lose their place in trade turnover. Also, it is possible to initially introduce a certain limit - for example, up to 3,000 euros per person - so that the digital euro does not turn into a complete investment instrument.

VII. Bulgaria and EUDI

Although no official statistical data are currently available, Bulgaria is steadily progressing toward the introduction of the European Digital Identity Wallet. Expected results from the implementation of the law include the deployment of a Bulgarian European Digital Identity Wallet, expanded access to electronic services, reduced administrative burden, and enhanced security and trust in electronic interactions across the EU [22]. These expectations align with findings from studies conducted across the Union. Research by the European Commission specifically examines which potential use-cases are considered most attractive by different segments of the EU-27 population [23]. The use-cases with the highest relative importance are linked to healthcare—namely accessing health records and using electronic prescriptions—followed by electronically signing personal documents and making payments through a digital wallet. Use-cases of high relative importance are generally consistent between women and men, with the exception of accessing important documents, which women rate as highly important and men as moderately important. More pronounced differences appear across age groups: while electronic prescriptions are rated as highly important among respondents over 50, payment through a digital wallet is rated as highly important among respondents aged 18–34 and 35–49 [23].

VIII. Conclusion

The introduction of a European Digital Identity Wallet (EUDI) is a serious step towards digital integration and legal digitalization in the EU [24]. It combines powerful technical mechanisms (MFA, SE/TEE) with the legal force of the qualified electronic signature (QES). However, the architectural solutions - device orientation, federated model, interaction with the digital euro - give rise to risks ranging from compromise of keys and vulnerabilities in the supply chain to systemic surveillance and social exclusion. The conclusion is that success

depends not only on cryptography, but also on the quality of implementation, transparency, independent audit and recovery and inclusion policies.

REFERENCES

[1] 2025 State of the Union Address by President von der Leyen, 10th September, 2025. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053. [Accessed: Dec. 15, 2025].

[2] 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, PE/68/2023/REV/1OJ L, 2024/1183, 30th April 2024. [Online]. Available: ELI: http://data.europa.eu/eli/reg/2024/1183/oj[Accessed: Oct. 26, 2025].

[3] (MFA) is a security process requiring users to provide two or more verification factors to gain access to an account, rather than relying solely on a password. By combining factors—something you know (password), have (smartphone), or are (biometrics)—MFA significantly reduces the risk of unauthorized access. [Online]. Available: https://trusted-digital-identity.europa.eu/eu-login-help/what-multi-factor-authentication-or-2fa_en [Accessed: Nov. 26, 2025].

[4] Secure Elements (SE) and Trusted Execution Environments (TEE), are foundational technologies for establishing a root of trust and protecting sensitive data in modern connected devices. "Hardware Security: Understanding the Differences Between a Secure Element, TPM, HSM, and a TEE", June, 13th 2025. [Online]. Available: https://tropicsquare.com/blogs/hardware-security-understanding-the-differences-between-a-secure-element-tpm-hsm-and-a-tee. [Accessed: Jan. 10, 2026].

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, pp. 1–88. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. [Accessed: Nov. 14, 2025].

[6] S. Pabst "EU Digital Identity Wallet Pilots Roll Out Under the Radar", October, 6th 2023. [Online]. Available: https://brownstone.org/articles/eu-digital-identity-wallet-pilots-roll-out-under-the-radar/?_gl=1*u4jcp6*_gcl_au*MTgxMzY3MDQwMS4xNzc0MTgwNjI4*_ga*MjEzMjc4NDc3My4xNzc0MTgwNjI4*_ga_P6T1TNYZ37*czE3NzQxOTEyNTEkbzIkZzAkdDE3NzQxOTEyNTEkajYwJGwwJGgw[Accessed March 3, 2026].

[7] A. Tomanová "EU chystávlastnídigitálnípeněženku do mobilu! Kdydorazí a co všemánabídnout?", 23.08.2025. [Online]. Available: https://www.letemsvetemapplem.eu/2025/08/23/eu-chysta-vlastni-digitalni-penezenku-do-mobilu-kdy-dorazi-a-co-vse-ma-nabidnout/. [Accessed Jan. 12, 2026].

[8] "Commission Implementing Regulation (EU) 2024/2979 — integrity and core functionalities of European Digital Identity Wallets". EUR-Lex. European Commission. 4 December 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj/eng[Accessed: Dec. 21, 2025].

[9] A. Kwiatkowska "Europe 2025: How Organisations Can Protect Data and Identity at Scale", 31 October 2025. [Online]. Available: https://www.keepersecurity.com/blog/2025/10/31/how-organisations-can-protect-data-and-identity-at-scale/ [Accessed Feb. 16, 2026].

[10] What is a level of assurance? eIDAS Levels of Assurance. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110081/eIDAS+Levels+of+Assurance.[Accessed: Feb. 13, 2026].

[11] EUDI Wallet: what are the mechanisms and guarantees of the trust model? 26 February 2025. [Online]. Available: https://www.idakto.com/blog/eudi-wallet-what-are-the-mechanisms-and-guarantees-of-the-trust-model/. [Accessed: Dec. 20, 2025].

[12] N. Tsakalakis, "Analysing the impact of the GDPR on eIDAS: Supporting effective Data Protection by Design for cross-border electronic identification through unlinkability measures", Thesis for the degree of Doctor of Philosophy, University of Southampton. 2020. [Online]. Available: https://eprints.soton.ac.uk/447268/1/N_Tsakalakis_PHD_WAIS_201120.pdf . [Accessed: Jan. 26, 2026].

[13] Digital death refers to the management, legacy, and transformation of a person's digital footprint—social media, cloud storage, emails, and assets—after they pass away. It covers legal, ethical, and personal issues regarding who owns, controls, or deletes this data, alongside the rise of digital, AI-generated memorialization and immortality. See also S. Pitsillides, M. Waller and D. Fairfax, "Digital Death: What Role Does Digital Information Play in the Way We are (Re)Membered?", In book: Digital Identity and Social Media, pp.75-90. July 2012. [Online]. Available: https://www.researchgate.net/publication/291811561_Digital_Death_What_Role_Does_Digital_Information_Play_in_the_Way_We_are_ReMembered [Accessed Jan. 12, 2026]. https://doi.org/10.4018/978-1-4666-1915-9.ch006.

[14] Personally Identifiable Data (PID or Personal Identifiable Information - PII) is any data that can distinguish, trace, or locate an individual's identity, such as names, Social Security numbers, biometric records, or combinations of data like date of birth and address. It is used to verify identity and is heavily protected by privacy laws to prevent fraud.[Online]. Available: https://www.ibm.com/think/topics/pii. [Accessed: Jan. 16, 2026].

[15] An Electronic Attestation of Attributes (EAA) is a type of digital document that confirms the accuracy of a specific attribute, such as a place of residence or professional qualification. Unlike the attribute itself, which is merely a data point, the EAA serves as an official, machine-readable document. It is issued by an authorized provider, guaranteeing authenticity and carrying the same legal value as its paper-based equivalent. An EAA can be added, stored and presented with the EU Digital Identity Wallet. [Online]. Available: https://www.digital-identity-wallet.eu/news/what-are-the-3-types-of-electronic-attestations-of-attributes-eaa/ [Accessed: Jan. 16, 2026].

[16] WSCD a highly secure, tamper-resistant hardware component designed to store, manage, and protect sensitive cryptographic assets like private keys, credentials, and biometric templates, specifically for digital ID wallets. See also "Is WSCD and WSCA described in European Digital Identity Wallet (EUDIW) ARF equivalent to SSCD?". [Online]. Available: https://www.methics.fi/is-wscd-and-wsca-equivalent-to-sscd/. [Accessed: Feb. 22, 2026].

[17] Architecture and Reference Framework (ARF) is a a set of common standards and technical specifications and a set of common guidelines and best practices. IT is a the main narrative text that describes the European Digital Identity Wallet and its ecosystem. See also "Version 2.0 of the Architecture and Reference Framework now available", 29th May 2025. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/900014854/Version+2.0+of+the+Architecture+and+Reference+Framework+now+available . [Accessed: Nov.20, 2025].

[18] ISO 18013-5:2021 is the international standard for mobile driver's licenses (mDLs), defining secure, interoperable technology for storing and presenting driver's licenses on mobile devices. It enables contactless verification via NFC, QR codes, or Bluetooth, ensuring high-level security, data integrity, and privacy-preserving,, user-controlled sharing. [Online]. Available: https://www.iso.org/standard/69084.html. [Accessed: Dec. 12, 2025].

[19] Qualified electronic signature (QES) is the most secure, legally binding electronic signature under EU eIDAS regulation, equivalent to a handwritten signature. It requires strict identity verification, a qualified certificate, and a secure signature creation device (QSCD). [Online]. Available: https://commission.europa.eu/system/files/2023-03/Instructions%20for%20QES%20signature%20of%20documents.pdf. [Accessed: Dec. 18, 2025].

[20] OpenID4VP is a protocol that extends the OpenID Connect standard, enabling users to securely present cryptographically verifiable credentials to prove their digital identity online without relying on passwords or traditional forms of authentication. [Online]. Available:

https://www.corbado.com/glossary/open-id-4-vp. [Accessed: Jan. 17, 2026].

[21] G.Belova and G. Georgieva Fake News as a Threat to National Security, International conference KNOWLEDGE-BASED ORGANIZATION, Vol. 24, Issue 1, pp. 19-22, June 2018. [Online]. Available: https://www.researchgate.net/publication/326653453_Fake_News_as_a_Threat_to_National_Security .[Accessed March 3, 2026]. https://doi.org/10.1515/kbo-2018-0002.

[22] T. Marinova and B. Popov Bulgaria Moves to Introduce European Digital Identity Wallet, Bill set for Public Consultation, BTA, 21.02.2026, [Online]. Available: BTA: Bulgaria Moves to Introduce European Digital Identity Wallet, Bill Set for Public Consultation Accessed: March 8, 2026].

[23] EUDI Wallet – NiScy – Comprehensive Use Cases and User Research Report DLV-03-02.01-08. [Online]. Available: What do Europeans want out of their EUDI Wallets New study sheds light - EU Digital Identity Wallet -. Accessed: March 8, 2026.

[24] A. Lozenska-Todorova, "Introduction of Digital Wallets in Bulgaria and the EU", International Politics, vol 2, 2024, pp. 91-115. А. Лозенска-Тодорова „Въвеждане на цифров портфейл в България и ЕС", сп. „Международна политика", бр.2, 2024, с. 91-115. [Online]. Available: http://ip.swu.bg/mod/data/view.php?d=1&advanced=1&filter=1&paging&page=1. [Accessed Feb. 23, 2026].