Trusted Economy Forum

ORGANIZER:

Trusted Economy Forum

PUBLISHER OF THE REPORT:

OBSERWATORIUM.BIZ

EUROPEAN DIGITAL IDENTITY FRAMEWORK

– what is it and how will it change the digital market?

Report prepared for the Trusted Economy Forum WEBINAR 2025

GOLD PARTNER:

asseco DATA SYSTEMS

SILVER PARTNER:

Authologic

Poczta Polska

HONORARY STRATEGIC PATRON:

COI Centralny Ośrodek Informatyki

HONORARY PATRONS: :

PIIT

CYFROWA POLSKA

MAIN FINDINGS OF THE REPORT

'EUROPEAN DIGITAL IDENTITY FRAMEWORK – WHAT IS IT AND HOW WILL IT CHANGE THE DIGITAL MARKET?'

WHAT MARKET, SERVICES AND ACTORS DOES THE EUROPEAN DIGITAL IDENTITY FRAMEWORK COVER?

- Notified electronic identification systems.
- Trust service providers established in the Union.
- Businesses using Strong User Authentication.

WHAT NEW SOLUTIONS AND SERVICES DOES IT INTRODUCE?

- European Digital Identity Wallet.
- Electronic attribute credentials.
- Electronic archiving of data and documents.
- Entering electronic data in the register.
- Managing remote electronic signature and seal creation devices.

WHAT WILL BE THE OBLIGATIONS FOR STAKEHOLDERS?

- Member States, public administrations, relying parties and trust service providers must implement procedures in line with the revised eIDAS Regulation, including registration, interoperability,data protection, incident reporting and compliance audit mechanisms.

WHAT NEW OPPORTUNITIES DOES THE EUROPEAN FRAMEWORK OF DIGITAL IDENTITY OPEN UP FOR THE MARKET?

- The European Digital Identity Wallet will enable the implementation of advanced services such as Strong Customer Authentication (SCA), digital onboarding (including Know Your Customer - KYC), secure payments, identity confirmation in transfers, digital representation of companies and sharing data for credit processes – all in a way that complies with EU regulations and maintains user control over data.

WHAT WILL THE EUROPEAN DIGITAL IDENTITY WALLET BE?

It will become a key identity tool across the EU. The wallet allows you to securely store and share identity data, apply qualified electronic signatures, and manage electronic attribute credentials. It will be available free of charge to EU citizens and residents for private purposes and will be mandatorily supported by all member states from the end of 2026.

Poland implements EDIW through the mObywatel application, which is undergoing a transformation to version 3.0.

The new version of the application will be compliant with with the amended eIDAS Regulation, will enable the creation of a qualified electronic signature and selective data sharing. Ultimately, it is assumed that the service will cover up to 20 million citizens.

Spis treści

1.Key objectives of the European Digital Identity Framework

1.1 What is the European Digital Identity Framework and what changes does it introduce?

July 2025 marks the eleventh anniversary of the publication of Regulation (EU) No. 910/2014 of the European Parliament and of the EU Council on electronic identification and trust services for electronic transactions in the internal market (the so-called eIDAS Regulation). The aim of the regulation was to harmonise the digital market – to create a unified legal and technical framework for digital transactions in the common market.

On February 29, 2024, the European Parliament voted on an amendment to the eIDAS regulation introducing a **European Digital Identity Framework**. On 26 March of the same year, the Council of the European Union also adopted this amendment. The accepted, amended regulation was published in the Official Journal of the EU in the following weeks, and twenty days after publication, i.e. on 20 May 2024, **it entered into force and is officially in force**. Full implementation is scheduled for the end of 2026.

The eIDAS Regulation of 2014 set out the conditions for the recognition by Member States of electronic identification means of natural and legal persons and established a legal framework for defined trust services. The European Digital Identity Framework provides an innovative approach to digital identity in Europe to ensure that European Union citizens and businesses have universal access to secure and trustworthy electronic identification and authentication.

The European Digital Identity Framework extends the scope of trust services provided, known from the previous regulation, with additional elements such as:

- **electronic attestation of attributes,**
- **electronic archiving of electronic data and electronic documents,**
- **management of remote devices for creating electronic signatures and seals,**
- **recording electronic data in the electronic register.**

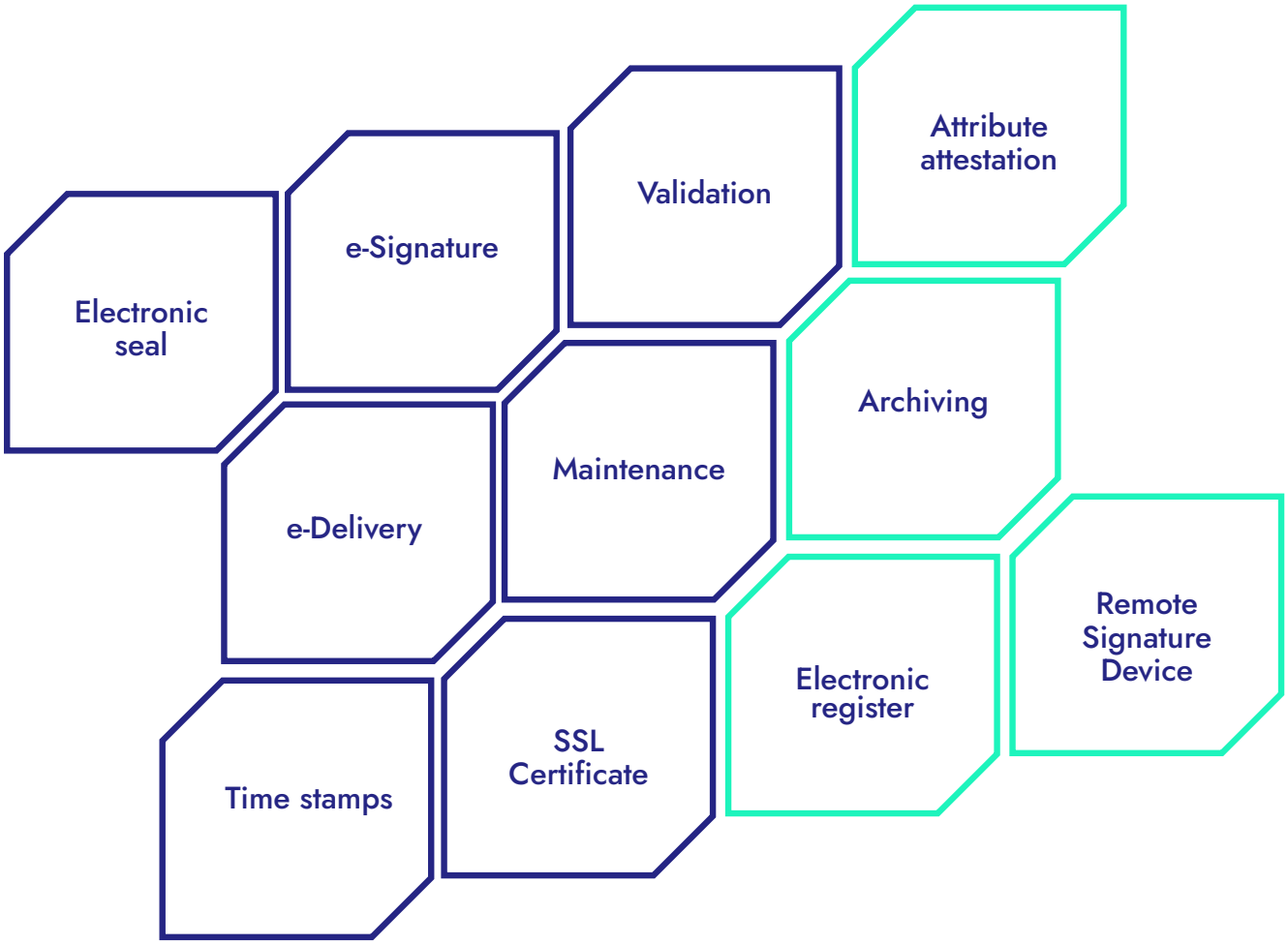

Figure 1. Existing and new trust services under the European Digital Identity Framework

The first executive regulations (also referred to as the implementing acts) defining the functions and requirements of security, as well as the shape of the new trust infrastructure resulting from the amended regulation, came into force in December 2024. Although some of the changes that come into force thanks to the amendment have already been reflected in the wording of the relevant regulations, others will have to wait until the relevant implementing regulations appear. The implementing acts, which are already in force as of 20.05.2025, concern the functioning of the European Digital Identity Wallet:

- **CIR 2024/2977** Commission Implementing Regulation (EU) 2024/2977 concerning PID (Person Identification Data) and EAA (Electronic Attestation of Attributes),
- **CIR 2024/2979** Commission Implementing Regulation (EU) 2024/2979 on integrity and essential functionalities,
- **CIR 2024/2980** Commission Implementing Regulation (EU) 2024/2980 concerning ecosystem notifications,
- **Commission Implementing Regulation (EU) 2024/2981 on the certification of portfolio solutions,**
- **CIR 2024/2982** Commission Implementing Regulation (EU) 2024/2982 concerning protocols and interfaces.

On 27 May 2025, four more implementing regulations will come into force on aspects such as:

- **CIR 2025/846** Cross-border identity matching of natural persons,
- **CIR 2025/847** Security incidents and breaches,
- **CIR 2025/848** Registration of relying parties,
- **CIR 2025/849** List of certified European digital identity wallets.

Whereas from 15 April to 13 May 2025, the European Commission collected public opinions on the third set of draft implementing acts, covering:

- **Procedural arrangements for peer reviews of electronic identification schemes to be reported to the Commission,**
- **Notification and verification of the commencement of the provision of qualified trust service,**
- **Verification of identity and attributes when issuing a qualified certificate or a qualified attribute credential,**
- **Qualified certificates of electronic signatures and electronic seals,**
- **Management of devices for remote qualified signature creation as a qualified trust service,**
- **Notification of qualified electronic signature and electronic seal creation devices that have been certified by certification authorities,**
- **Validation of qualified electronic signatures and seals as well as advanced electronic signatures and seals,**
- **Qualified validation services for qualified electronic signatures and seals,**

- **Qualified maintenance services of qualified electronic signatures and qualified electronic seals,**
- **Provision of qualified electronic time stamping services,**
- **Requirements for qualified registered electronic services,**
- **Submission of annual reports by supervisory authorities to the Commission.**

Before publication, the drafts of these acts will undergo a thorough modernization.

REPORT EXPERT

ROBERT POZNAŃSKI
ANALYST, ASSECO DATA SYSTEMS

The eIDAS 2.0 Regulation is a natural evolution of the first Regulation on electronic identification and trust services adopted back in 2014.

The first Regulation focused primarily on trust services and only introduced electronic identification as a new service. eIDAS 2.0 expands and organizes the mechanisms of electronic identification, which should make these services more transparent and their implementation easier for citizens.

One of many innovations is the introduction of the EUDI Wallet, which addresses the changing lifestyles, more frequent travel, or use of digital services at the cross--border level.

In order to improve the implementation of digital identity wallets, pilot programs are being implemented between different countries. They involve, for example, public administration and commercial entities, thanks to which it will be possible to meet the expectations of both the implementing entities and the people who will use these solutions in the future.

1.2 Digital Identity Wallet

The most recognizable and most important change introduced by the European Digital Identity Framework is a tool called the European Digital Identity Wallet.

The European Digital Identity Wallet
is an electronic identification means that allows the user to securely store and validate data identifying a person as well as electronic attestation of attributes. In addition, it enables the secure management of this data and credentials for sharing with relying parties and other users of European Digital Identity Wallets that enable qualified electronic signatures or qualified electronic seals.

The aim of the identity wallet is to strengthen the European Single Market by enabling citizens, residents and businesses to identify and authenticate both online and offline. It is assumed that it will be possible to refer to the European Digital Identity Wallet as a tool that is:

- secure – will ensure data storage and sharing through secure communication protocols,
- trusted – will be treated as a reliable source of data,
- user-friendly, convenient and accessible – thanks to a simple and intuitive interface, created with users in mind,
- accepted throughout the European Union – will give the possibility of identification in all EU member states.

The regulation sets a deadline for the obligatory introduction of the wallet and making it available to the users – EU member states must have their own digital wallet accessible for citizens, entrepreneurs and other institutions no later than 30 months after the entry into force of the European Digital Identity Framework. Users will be able to easily prove their identity and share electronic documents from their digital wallets using their mobile phones and other channels, as well as confirm their attributes (e.g. professional

qualifications or possession of a driver's license). The wallet will be an official means of identification that will be used in the public and private sectors. It will also offer a built-in qualified electronic signature, which is to be available to every natural person and free of charge when used for private purposes.

In Poland, the role of the European Digital Identity Wallet will be played by the mObywatel application, already known on the Polish market.

REPORT EXPERT

MICHAŁ TABOR

PARTNER, MEMBER OF THE BOARD, OBSERWATORIUM.BIZ
EXPERT IN IDENTIFICATION, VERIFICATION AND ELECTRONIC SIGNATURE, PIIT

The idea of a digital identity wallet for people is now well-known. It usually works as a mobile app that lets users share their verified identity information. The eIDAS regulation also introduces a wallet for legal person, called a business wallet. This could help speed up digital changes in both business and government. One of the first uses of the business wallet will be to manage authorizations and powers of attorney, for example in Know Your Business processes. At first, company-related data might appear in personal wallets, but later it will move to the business wallet. This wallet can help consolidate multiple separate systems into a single, transparent, and shared system for managing roles and access . Over time, the business wallet can help automate business tasks by allowing secure sharing of company data, useful information and proving that business details are real. I am confident that the business wallet will become a regular part of electronic transactions in the coming years.

1.3 Other new services of the European Digital Identity Framework

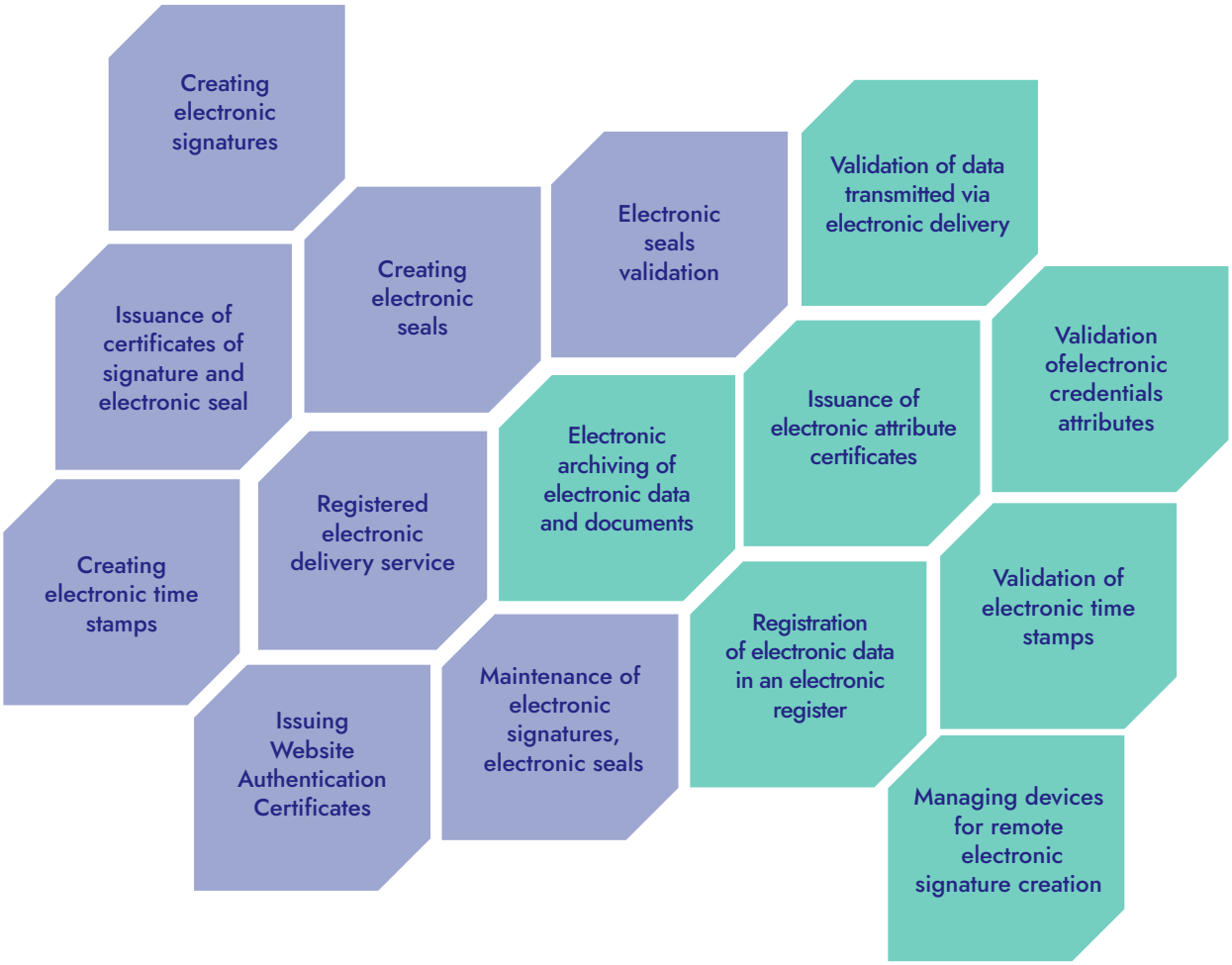

Figure 2. Current and new solutions based on trust services

The European Digital Identity Framework allows for the introduction of a number of new solutions based on trust services. These include electronic archiving of electronic data and documents, validation of data transmitted via e-deliveries, issuance of electronic attribute credentials and their validation, recording of electronic data in an electronic register, validation of electronic time stamps, as well as remote management of electronic signature creation devices. The following are descriptions of some of the new services:

Electronic attribute confirmations

The European Digital Identity Framework introduces qualified electronic attestation of attributes, which is an electronic attestation of attributes issued by a qualified trust service provider that meets certain requirements. Electronic attribute confirmations are digital documents or certificates that verify specific properties, characteristics, or permissions assigned to a person, organization, or object. They are issued by trusted institutions or entities that can confirm the veracity and authenticity of these attributes. Electronic attribute assertions can be used in a variety of contexts, such as:

- digital identity: confirms the person's identification data, such as name, surname, identification number or address,
- horizations and qualifications: verify professional qualifications, authorization to perform specific activities or possession of specific licenses,
- organizational attributes: confirm roles and positions in organizations, e.g. employee, board member or representative,
- product properties: confirm the characteristics and specifications of the products, e.g. quality certificates, compliance with standards.

Electronic attribute assertions are a key component of the new trust infrastructure, enabling information to be verified securely and efficiently both online and offline. Examples of use include onboarding into financial services, logging into IT systems, authorizing transactions, or confirming qualifications during recruitment. Thanks to the European Digital Identity Framework, electronic attribute confirmations gain a unified legal framework in the European Union, which will increase their credibility and interoperability on the European market. Electronic attribute authentication will be recognized by courts and authorities, and every user will be able to use the Digital Identity Wallet to receive, store, and share electronic attribute credentials.

Electronic archiving as a trust service

Electronic archiving is a service that involves receiving, storing, retrieving and deleting data and electronic documents, ensuring their durability, legibility, integrity, confidentiality and proof of origin throughout their storage period. Currently, electronic archiving in the European Union countries operates based on national regulations, which makes it impossible to provide and recognize this type of services across borders. By integrating this service into the European Digital Identity Framework, a unified European approach is being created that avoids market fragmentation and can increase demand for this service across the EU. However, this comes with specific requirements for trust service providers. They must use procedures and technologies that ensure the durability and readability of electronic data over time, as well as its integrity and accuracy from storage to retrieval

1.4 Responsibilities of stakeholders

The amendment to the regulation in question not only introduces new services and solutions but also sets out detailed obligations for individual stakeholders of the European digital market. Existing and new market players, Member States and their administrations, will have to face the challenges posed by the European Digital Identity Framework. Users will face many challenges connected with the acceptance and understanding of the new services and the conditions of their functioning.

Obligations of the Member States

The Member States of the European Union are responsible for ensuring that their citizens and residents have access to one or more European Digital Identity Wallets that meet harmonised EU standards for security, interoperability and protection of personal data. This obligation includes both the creation of national mechanisms for the certification and supervision of portfolio providers and ensuring their mutual recognition across the Union. Member States must also guarantee equal access to electronic identification services for all citizens and residents – regardless of their origin, social status or location – by removing digital and technical barriers. Importantly, the use of the wallet cannot be mandatory; Member States are required to provide alternative means of identification when dealing with public administration. Member States are also required to establish electronic registers of parties which trust the wallets, together with national registration policies that set out, among other things, the notification process, documentation, verification method, procedures for updating data and redress mechanisms. In addition, countries should also conduct educational and information activities, support

the development of digital competences of citizens and initiate pilots of innovative solutions through the so-called regulatory sandboxes, which enable safe testing of new technologies in a limited environment.

Responsibilities of public administration

Public administration institutions, both at a national and local level, have a duty to fully recognise and support the use of European Digital Identity Wallets as a means of identification and authentication in electronic public services. This means adapting IT infrastructure and administrative procedures to handle the wallet when serving citizens and complying with the EU principles of data minimisation and privacy. Public administration institutions cannot deny access to services because a citizen does not use the wallet or favor digital wallet users over others. At the same time, they should actively cooperate with their suppliers, ensuring an effective process of registration of relying parties and control over their compliance with the law. If irregularities are found, the administration is obliged to take supervisory and corrective actions.

Obligations of relying parties (businesses and digital platforms)

Companies providing digital services, especially in regulated or highly authenticated sectors, are required to accept European Digital Identity Wallets where such authentication is required by EU, national or contractual law. This is particularly the case for very large online platforms, which are obliged under the DSA (2022/2065) to allow users to use European Digital Identity Wallet as a login method if the user requests it. Businesses must ensure that user requests for data comply with the principles of proportionality and necessity and clearly define what data is required and for what purpose. It is also the responsibility of the relying parties (private companies) to register in the national registers, conduct data protection impact assessments and ensure compliance with the GDPR – including the processing of special categories of data, such as health data. Registration must be transparent, non-discriminatory and adapted to different business models – both online and offline. The registers are intended to allow the user to verify the relying party and its permissions. Relying parties should only use the wallet to the extent that they have previously notified and that has been approved by the registrant.

Obligations of the European Digital Identity Wallet providers

European Digital Identity Wallet providers, whether public, private, acting under the authority of a Member State or independently, have a responsibility to implement the highest standards of security and privacy starting from the design stage of the service. They must ensure that the data related to the handling of the wallets is fully logically (and preferentially physically) separated from the rest of the data processed by the organization. Vendors are not allowed to collect data about the user's transactions, their content, or their history unless they give their prior, informed, and explicit consent to do so. The functionality must include a clear management panel, selective data disclosure, the ability to manage pseudonyms, and the default inclusion of transaction history tracking, including the option to delete them. Providers must also ensure that the user can transfer their data to another wallet at no additional cost, and that their software must be interoperable with mobile devices and platforms (e.g. NFC, secure elements, SIM).

Obligations of trust service providers

Trust service providers, especially those issuing qualified certificates and electronic attestations of attributes, are subject to new, precisely defined obligations under both the eIDAS Regulation and the NIS2 Directive. They must implement adequate technical and organizational measures to manage cybersecurity risks and report incidents that may affect the quality of services provided. Particular emphasis is placed on the need to provide „complete certainty" when verifying the identity of persons to whom qualified certificates or attestations are issued. To this end, various authentication methods are allowed, including the combination of mid-level electronic identification means with additional verification mechanisms. In the case of qualified attribute attestations, providers must enable verification of these attributes against authentic sources, in accordance with the provisions of EU or national law. In addition, the European Digital Identity Framework introduces new regulations on penalties for trust service providers in the event of a breach of the security of the services they provide. Additional requirements and penalties apply to both qualified and non-qualified trust service providers.

Entitlements and opportunities for users (EU citizens and residents)

Users of European Digital Identity Wallets, i.e. citizens and residents of the European Union, will not have any new obligations, but they will gain a number of rights and control over their personal data. The digital wallet must remain under their sole control, and its use must be completely voluntary. Users have the right to link, store, selectively share, and delete the data contained in the wallet. They should also be able to create and manage pseudonyms and have access to a complete history of transactions carried out using the wallet. By default, the wallet is to enable the submission of qualified electronic signatures without the need to undergo additional administrative procedures and free of charge (in non-professional applications). If misuse or an unlawful data request is detected, the user should be able to report the incident to the DPA directly from the wallet application. In addition, the European Digital Identity Wallet will also be available for use outside the user's home country throughout the EU. EU citizens and residents will be able to exchange digital information related to their identity, such as their address, age, professional qualifications, driving licence and other permits and payment details, in a secure manner and with a high level of data protection.

1.5 Timetable

As mentioned above, the regulation introducing the European Digital Identity Framework officially entered into force on 20 May 2024, and the first five implementing acts entered into force on 24 December 2024. Each Member State is obliged to provide its citizens with at least one European Digital Identity Wallet within 24 months from the date of the publication of the above-mentioned implementing acts, which in practice means 24 December 2026.

Current qualified trust service providers must adapt their infrastructure and services to the requirements of the amended regulation and submit an appropriate compliance audit report no later than May 21, 2026.

From December 24, 2027, regulated industries must accept European Digital Identity Wallets as an authentication method. This applies to companies operating in sectors where strong authentication is required by law, such as banking, telecommunications and government services.

Figure 3. Timeline for the implementation of the European Digital Identity Framework

1.6 European Digital Identity Wallet pilots

In 2023, the European Commission commissioned a task called Large Scale Pilots (LSPs) for EU Digital Identity Wallet. These pilots were launched to test in practice, at scale and in real-world conditions, how the wallet will perform in an ecosystem of real services, providers and use cases. In the first phase of the program, planned for a period of two years (2023-25), four international pilot projects were created, in which dozens of commercial organizations, entities from public administration as well as the scientific world from all over Europe participated:

- POTENTIAL,
- EU Digital Wallet Consortium (EWC),
- NOBID Consortium,
- DC4EU (Digital Credentials for Europe).

The task of these projects is to implement and test real business scenarios using the wallet, in areas such as, among others:

- travel and airport check-in,
- opening a bank account,
- signing documents,
- access to health and education services,
- confirmation of professional qualifications and legal representation.

The above-mentioned consortia will cease operations in the summer of 2025. At the beginning of 2025, as a result of another tender, two new consortia were selected, namely: WE BUILD (Wallet Ecosystem for Business & Payment Use cases, Identification, Legal person representation, and Data sharing) and Aptitude. Both new projects are expected to start in September 2025 and run for two years.

According to the amended eIDAS Regulation, Member States will be required to issue the wallet by 2026. The pilots serve as a transitional stage, allowing testing and experience before full implementation.

Używaj narzędzi ekosystemu
#EnterprisePaperless!

Transformacja cyfrowa zwiększa efektywność, ale wymaga gotowości do zmian w procesach i sposobie myślenia. Dzięki nam odkryjesz korzyści z przejścia na paperless i przeniesiesz swoją organizację do cyfrowej przyszłości, gdzie papier przestaje być nośnikiem dokumentów.

e-Doręczenia

Wysyłaj elektroniczne listy polecone

SignHub

Podpisuj e-dokumenty z osobami spoza organizacji

Signer

Buduj i wdrażaj procesy paperless

WebNotarius

Dbaj o bezpieczeństwo e-dokumentów

Usługi zaufania

Chroń i zabezpieczaj e-dokumenty

e-ID Hub

Potwierdzaj tożsamość online

Dołącz do świadomych przedsiębiorców.
Sprawdź jak na: paperless.asseco.com

asseco

2. Implementation of the European Digital Identity Framework in Poland

2.1 Alignment of mObywatel 2.0 with the European Digital Identity Wallet

The mObywatel 2.0 application is Poland's flagship digital identity solution, enabling citizens to access and manage a wide range of official electronic documents directly from their smartphones. The app currently supports key documents such as the digital ID (mDowód), driving licences, vehicle registration data (mPojazd), student and pensioner ID cards, and the Large Family Card, all in electronic format. These digital credentials are legally recognized and widely accepted by both public and private sector entities.

Document verification within mObywatel 2.0 is designed to be user-friendly, secure, and versatile. Two primary verification methods are available: visual verification, which involves checking the document's layout and security features such as holograms and dynamic backgrounds; and cryptographic verification, which relies on public key infrastructure (PKI) as the backend trust framework. In this model, time-limited QR codes are used to initiate the engagement between the user and the relying party, enabling secure data exchange. The QR code facilitates the session, while PKI ensures the authenticity and integrity of the transmitted data, without storing any personal information on the verifier's side.

All user data is encrypted and stored along with cryptographic keys in the protected environment of the mobile device. The data shared is only displayed for a short period of time and cannot be saved by the verifier, which ensures privacy and minimizes the risk of misuse.

Despite the high level of technological maturity and a wide range of functionalities, the mObywatel 2.0 application is not yet fully compliant with the amended eIDAS regulation. Below is a comparison of mObywatel 2.0 with the target application version 3.0.

Feature	mObywatel 2.0	mObywatel 3.0 (Polish Digital Identity Wallet)
Security level	Substantial	High or Substantial+
Safety Certification	Not required	Required accordance with Common Criteria
Qualified electronic signature	No	Yes
Mobile documents	Static dataset	Selective disclosure by the user
Relying Parties Integration	Manual administrative procedures	Automatic integration based on earlier registration

The Centre for Information Technology (COI – Centralny Ośrodek Informatyki) is already upgrading mObywatel to the EUDI Wallet. By developing the solution internally, COI minimizes external dependencies and strengthens the state's long-term technological independence. The solution fully complies with the adopted European implementing acts and related technical specifications. It supports credential formats defined in the Architecture Reference Framework.

To ensure cross-border interoperability, COI actively tests the solution in EU pilot initiatives. Notably, COI participated in the Warsaw Interop Event in February 2025, where it joined international tests to validate technical and legal compatibility with other national implementations of the European Digital Identity Wallet. These efforts demonstrate the readiness of the Polish solution to operate within the European ecosystem of trusted digital identity services.

2.2 National pilot of a qualified electronic signature integrated with mObywatel 2.0

The Polish Ministry of Digital Affairs is running a pilot based on mObywatel 2.0, where the wallet confirms the identity of the person signing a document. The signature process uses a one-time qualified electronic signature. Starting in October 2025, the pilot will involve all Polish Qualified Trust Service Providers and aim to offer qualified signatures free of charge to natural persons for personal, non-professional use.

The initiative aims to deliver a smooth and secure signing experience by using mObywatel 2.0 as the onboarding tool, while qualified trust service providers (QTSPs) handle certificate issuance and signing. QTPS integrated with mObywatel 2.0 will issue the certificates, and users can select one of them from a randomized list of providers to ensure fairness. Users authenticate themselves with their national e-ID card and the mObywatel app. The system applies signatures using one-time certificates and ensures compliance with the PAdES standard for document signing. Signed documents will be immediately returned to the initiating platform.

This pilot is underpinned by formal agreements between the Ministry of Digital Affairs and all involved QTSPs, setting clear terms for cooperation, data handling, and responsibilities. The state provides technical and legal coordination to ensure a scalable, sustainable service model aligned with the future regulatory needs.

The pilot lays the foundation for Poland's long-term integration of qualified e-signatures into the EUDI Wallet ecosystem. It not only tests technical and legal readiness but also prepares for wide-scale deployment that meets user needs and EU obligations, while strengthening trust in national digital services and promoting their use.

2.3 Market Collaboration in Trust Services: Relying Party Onboarding to Access Electronic Attribute Credentials

According to the eIDAS 2.0 regulation, all EU member states that implement the European Digital Identity Wallet are required to establish a national system for the registration of relying parties. These are entities that want to use the wallet to verify the identity of users or obtain data from them in the form of various attribute credentials. The registration system must include, among others, the method of registering entities in the country of their registered office, the rules for issuing access certificates confirming their access rights and the mechanisms for managing these certificates over time. Information on registered entities should be publicly available – both in a human-readable form and in a form that can be processed automatically (e.g. via a website or API). Each Member State should publish a national policy in this area. This policy should allow for a quick and automated registration process. The whole process must be user-friendly and available online. According to the draft EU implementing act, this process should be inexpensive and proportionate to the level of risk.

The draft of the European standard ETSI TS 119 475 provides for two models for the implementation of this process:

- The first model is based on the handling of the process by public administration – the entire process of registration and issuance of access certificates is carried out directly by a state institution, such as the Ministry of Digital Affairs. The state retains full control over the process of verifying entities, but this model requires the construction of dedicated infrastructure and the involvement of appropriate human resources.
- The second model assumes the delegation of tasks to qualified trust service providers. It is them, on the basis of agreements and national regulations, who conduct the process of registration and issuance of access certificates on behalf of the state. This model allows the use of the existing infrastructure and QTSP expertise, thus relieving the burden on public administration and reducing operational costs.

The decision regarding the choice of a specific model in Poland has not yet been made. Work is underway to determine the final solution.

2.4 Target model for a qualified electronic signature based on the European Digital Identity Wallet

Poland's target model for qualified electronic signatures (QES) in the EUDI Wallet focuses on delivering the capability to all natural persons free of charge. The service will be available exclusively through the national digital wallet (mObywatel 3.0) and aims to ensure simple, secure, and legally recognized digital signing for personal, administrative, and business-related transactions initiated by the state.

The model covers three basic usage scenarios:

- Citizen-to-Citizen (C2C) – signing documents in private contacts, based on short-term certificates issued remotely for the duration of one signature session,
- Citizen-Administration (C2A) – signing of official documents, with full integration of the identification and signature process with public administration platforms,
- Citizen-Business (C2B) – the use of signatures in contacts with private entities with full integration of the identification and signature process with commercial platforms.

Depending on the selected financing model, limitations on the number of signatures may be introduced. It is currently assumed that C2C interactions remains free of charge. Other use cases may require a more nuanced financial approach to support the sustainable development of the trust services market. Several funding models are being explored, including annual subscriptions per user, flat-rate subsidies for providers, or per-signature pricing. In C2A scenarios, the cost might be covered by the state, while in C2B cases, businesses initiating the process could potentially bear the cost of signing.

Ultimately, the solution aims to achieve mass adoption, targeting 20 million users by 2031. It ensures the availability of qualified signatures as a basic digital service, strengthens citizen access to digital administration, and supports trusted digital interactions across sectors, while preserving market competition among trust service providers.

RAPORT EXPERT

RAFAŁ SIONKOWSKI

**DEPUTY DIRECTOR OF THE DEPARTMENT OF DIGITAL CHANNELS,
CENTRAL INFORMATION TECHNOLOGY CENTER (COI)**

In response to the requirements of the European eIDAS 2.0 regulation, we are developing a new version of the mObywatel application – a digital identity wallet compliant with the latest standards for electronic identification and trust services. This initiative presents a significant challenge, both technologically and organizationally – especially considering that Poland already operates an advanced and widely adopted solution. In many respects, we face more complex challenges than countries that are building their systems from scratch – including the migration of user data and experience for over 9 million active users.

A comprehensive implementation of the European digital identity has the potential to benefit not only public administration but also the entire economy. New mechanisms for digital identification and authentication will accelerate the digitalization of processes, enhance the security of online services, and simplify citizens' interactions with institutions.

To ensure that the implementation of eIDAS 2.0 delivers the expected results, close cooperation between public and private entities is essential. Ensuring interoperability between state-run solutions and the commercial market is of particular importance, especially in the context of qualified electronic signatures. In an environment where the trusted signature is already a public tool, a broad consensus is needed between qualified trust service providers, the private sector, and government institutions to ensure consistency, security, and wide availability of digital identity services.

Poczta Polska

POLECONY

CZY WIESZ, ŻE...

e-Polecony do księgowej

wyślesz na luzie w czasie pracy?

Załóż adres do doręczeń elektronicznych i korzystaj z e-Poleconego:

- wygodna wysyłka z dowolnego **miejsca i urządzenia**
- **bez awizo**, bez kolejek
- gwarancja **bezpiecznego** szyfrowania
- **automatyczne** generowanie dokumentów
- możliwość **monitorowania** listu
- **ochrona środowiska** przez redukcję papieru

Dowiedz się więcej na **www.e-polecony.com**

3. Benefits and new market opportunities resulting from the European Digital Identity Framework

The European Digital Identity Framework aims to revolutionise the way citizens and businesses operate in the digital environment. The central element of the amended regulation is the European Digital Identity Wallet, described in detail in the previous part of the report. Thanks to it, users will gain a tool that allows for a safe and easy management of their digital identity, as well as enables the implementation of several processes both on-line and on-site, which have so far been time-consuming and burdened with the risk of errors. The wallet will offer a wide range of benefits and real opportunities for business and administrative practice in the digital, integrated EU market. However, its effective functioning will only fully manifest itself in the context of the entire ecosystem, in which it will function together with the sources of attributes, the wallet acceptance network and the transactions it will enable.

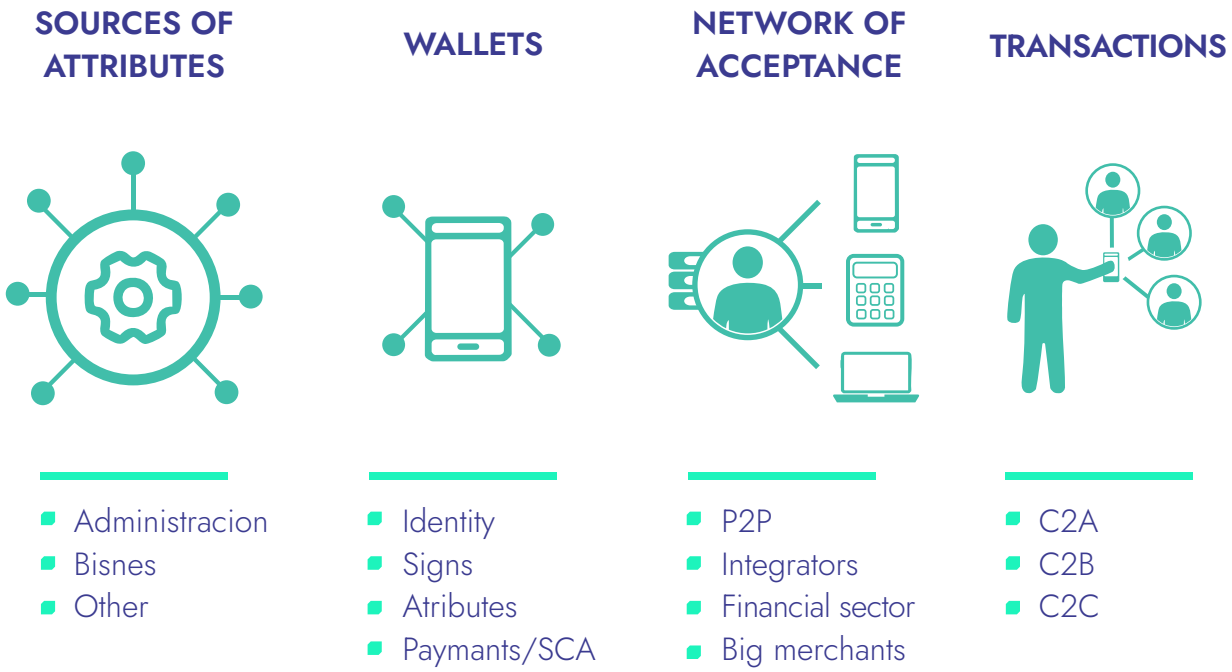

Figure 4. European Digital Identity Framework Ecosystem

A functioning ecosystem will allow the following benefits and new values to emerge for its participants:

Common, cross-border and secure identification of individuals and companies in the online and offline environment

Digital identity wallets will comply with established EU technical standards and will provide the same user experience and set of functionalities regardless of the country of issue. They will enable secure authentication and identification in public and private services – both at home and abroad. The introduction of solutions such as automatic filling of electronic forms and the „once-only" principle will reduce handling time and the risk of errors.

The wallet will be able to store and share identity attributes such as employment status, place of residence, eligibility for discounts, valid tickets, tax payment information, and proof of ownership. In the future, it will also be possible to securely store travel documents (e.g. passports, visas), which will facilitate airport check-in and check-in at hotels.

Unlike current eID systems, the wallet user will have full control over their data – they will know who has received certain information and for what purpose, and will also be able to withdraw consent to its further sharing.

The European Digital Identity Wallet will enable user identification by private service providers (e.g. banks), authorisation of online payments and remote opening of bank accounts without the need to visit a branch. In addition, the user will be able to confirm the representation of the entity (e.g. company) in business contacts.

The wallet will also include mechanisms to confirm the identity of the other party and record the history of data sharing. All transactions will be compliant with the eIDAS regulation, which will significantly increase security and trust in the digital environment.

Qualified electronic signature for everyone

Each wallet user will have access to a qualified electronic signature, enabling the signing of documents – including employment contracts – with full legal force. This signature will be available at no additional cost or unnecessary administrative formalities.

Enhancing cybersecurity and coherence with the EU's digital policy

The eIDAS 2.0 regulation is a part of the EU's broader strategy „Path to the Digital Decade 2030", which assumes building a secure, trusted and integrated digital environment. The wallet will support users in protecting their data and identities from misuse, ensuring compliance with the GDPR and other EU cybersecurity regulations.

New opportunities for users and business

With the European Digital Identity Framework, businesses will be able to lawfully provide high-trust services across the Single Market, while minimising the costs associated with national differences in electronic identification. Examples of wallet usage scenarios will include:

- Strong Customer Authentication (SCA) – the wallet can act as a tool enabling strong authentication in accordance with the requirements of PSD2 and eIDAS, which will be crucial when authorizing electronic payments and logging in to banking services,
- Implementation of the KYC (Know Your Customer) function in financial processes – onboarding to financial services (banking or insurance), or verification of customers making cash deposits to self-service or POS devices, where the user will be able to confirm their identity digitally, without the need to show a physical document,
- Making payments using the wallet with the use of attributes such as age or right of entry (e.g. transport tickets or tickets for sports and cultural events),
- Verification of the recipient's data – the wallet will be able to help confirm the identity and correctness of the recipient's data for financial transactions, which will reduce the risk of errors and fraud,
- Transfer of data to the credit process – data necessary to assess creditworthiness (e.g. about employment, income, liabilities) will be able to be transferred through the wallet in a secure and confirmed manner,
- Identity wallet for companies – companies will be able to use a version of the wallet designed for legal entities, which will allow, for example, employees to confirm the company's representation in commercial or administrative transactions.

REPORT EXPERT

PIOTR STERCZAŁA

PARTNER, MEMBER OF THE BOARD, OBSERWATORIUM.BIZ

The implementation of the European Digital Identity Framework will be a fundamental shift, not only in regard to electronic identification but also in other business and administrative processes – both online and offline. These new regulations, and more importantly their implementation and practical application, will open a completely new chapter in the digital transformation of the European Union.

Under this regulation, European Digital Identity Wallets will be introduced to the public, enabling secure and convenient identification across all EU member states. EUDI wallets have become a symbol of the changes introduced by eIDAS 2.0, as they aim to provide universal access to digital identification, qualified electronic signatures, and verifiable attributes. In my view, however, attributes will be the truly revolutionary element of the upcoming changes.

By leveraging attributes, individuals – and ultimately also legal entities – will be able to share virtually any personal or organizational information with other parties in a secure, streamlined, and fully controlled manner. The ability to digitize and transfer wide array of data via attributes will serve as a catalyst for unprecedented growth in transactional activity, both at the local and European levels. New processes – previously difficult or even impossible to implement – will become feasible, while existing ones will become more convenient, efficient, and above all, secure.

Authors of the report:

Sławomir Hadryan,
Dominika Rzęsa,
Michał Tabor,
Piotr Sterczała,
Miłosz Brakoniecki,
Marcin Wolski.

Legal notice

The opinions contained in the report were issued on the basis of knowledge gained from market research and the experience of the authors of the report. The authors do not take responsibility for decisions made on the basis of opinions issued as part of the report „The European Digital Identity Framework – what is it and how will it change the digital market?"

CONSULTING WORKSHOPS ANALYTICS

www.obserwatorium.biz

#electronic_signature
#trusted_services
#eID
#digital_services_design
#digital_transformation

OBSERWATORIUM . BIZ