REPORT PUBLISHER:

OBSERWATORIUM.BIZ

GOLD PARTNER:

asseco DATA SYSTEMS

Trusted Economy Forum

Report

REMOTE IDENTITY PROOFING, E-SIGNATURE AND E-SEAL

IN BUSINESS PRACTICE

SILVER PARTNER:

Namirial · Procivis AN ORELL FÜSSLI COMPANY · Authologic · Poczta Polska · aruba.it

BRONZE PARTNER:

KIR · SIGNIUS · TRUST LYNX · billon · IDENTT

REMOTE IDENTITY PROOFING, E-SIGNATURE AND E-SEAL IN BUSINESS PRACTICE

in questions and answers

What is remote identity proofing, and what business needs does it address?

- It enables acquiring individual and business clients online securely without requiring physical contact.
- In the Polish market, common methods include the Trusted Profile, Personal Profile, mObywatel app, video verification, biometric technologies, and the mojeID service.
- The main sectors adopting this technology are finance, insurance, telecommunications, and public administration.
- The upcoming European Digital Identity Wallet will allow storing identity data and attributes, securely sharing them, and expanding the practical business use of remote identity proofing.

What do qualified electronic signatures provide?

- They are a legally binding form of signature equivalent to a handwritten signature.
- Key applications include signing contracts, financial documentation, and business agreements, meeting cross-border requirements.
- Solutions from Polish and other European qualified providers operating under the eIDAS regulation are acceptable.
- Cloud-based solutions are gaining significance, enabling remote issuance and use of signatures while integrating them into business processes.

What are electronic seals, and when should they be used?

- A qualified electronic seal, as defined by the eIDAS regulation, confirms the authenticity and integrity of electronic documents.
- e-Seals are widely used in both public and private sectors, allowing institutions and companies to legally secure documents.
- This service supports process automation, such as contract signing or invoice issuance, accelerates the flow of digital documents, eliminates the need for physical seals, and reduces operational costs.

Table of contents

Purpose and scope of the report

The aim of this report is to provide knowledge on the methods of remote identity verification, qualified electronic signatures and qualified electronic seal available on the Polish market, with an emphasis on their business use. The scope of the report includes an overview of key tools and solutions, their legal bases and recommendations regarding the use. The developed material contains information useful for entrepreneurs and organizations implementing digital processes. In addition, the report has been expanded to include examples of the use of these services in individual sectors (use-cases).

1. Remote customer identity proofing in digital processes

The possibility of acquiring customers remotely has already become a must for entities from all industries and areas of business activity. The digitization of subsequent processes of everyday life allows users, consumers and citizens to handle more and more matters electronically. At the same time, companies can save money on reducing the costs of building and maintaining a network of customer service points and resign from methods that require the transfer of paper documents, e.g. using a courier. Younger generations even prefer the possibility of remote contact and „on-boarding" via a mobile or web application, considering a visit to a branch or telephone contact as less preferred.

In the **process of remote onboarding**, when there is no physical meeting and no presentation and verification of the identity document in the traditional way, it is crucial for both parties to the transaction that the identity of the applicant is recognized in a proper, safe and ergonomic manner. It is also important that the party relying on the data presented is given the highest possible certainty that it relates to the right person.

Identity proofing (verification) is crucial for trust in all digital services that require the identification of a natural or legal person. This is the process by which the service provider **collects and verifies** information about **the applicant** and verifies that the information collected and validated actually belong to the applicant who uses it under their control.

Currently, various remote methods are widely used, enabling quick and secure confirmation of the identity of new customers. They are provided for many services remotely, without the need to visit the branch personally.

1.1. Methods of remote proofing of customer identity

The available and most common methods of validation identity are discussed below. The main factors influencing the choice of the method of identity proofing are:

- legal requirements of the service and the method of verifying customers, e.g. related to anti-money laundering regulations;
- requirements of the user environment using the service, e.g. mobile application, website, availability of a camera or readers;
- requirements of the course of the process, including its duration;
- security requirements, including risks and possible losses in the event of incorrect identity confirmation.

Remote identity confirmation methods have been successfully implemented in many industries, but they are particularly commonly used in financial services – banking, insurance, loan or investment services. Identity confirmation is also successfully used in games of chance, telecommunications and media (i.e. electricity, gas). Remote identity confirmation is successfully used in all public services available electronically.

The available remote identity confirmation solutions are:

1) State-provided means of identification which is one of the key methods for secure access to public and private services. In Poland, the tools that meet this criterion are:

a. Trusted Profile – notified in the EU at the average substantial level of assurance, available only for the needs of public services – based on login, password, SMS code or electronic banking systems;

b. Personal Profile – notified in the EU at a high level of assurance – based on an ID card and PIN number – available for the public and private services;

c. The mObywatel profile – a national means of identification at the substantial level of assurance – based on the mObywatel application – available for the public and private services.

2) Means of identification provided by commercial entities – on the Polish market operating as the mojeID solution provided by the National Clearing House (KIR) and based on the identity of the electronic banking customer. Banks have extensive systems for verifying their customers that meet the requirements of anti-money laundering regulations, and undergo additional audits of compliance of electronic funds management processes. Banking electronic identification means can be used by private and public sectors.

3) Video call with the operator – allows you to follow the process of confirming your identity carried out personally by showing an identity document to the camera and confirming its compliance and the use of the document by the owner. The entire identity verification process is conducted and supervised by the operator, who confirms the verification of the identity document as well as the use of the document by the owner. The method is also supported by the automation of downloading data from the document (OCR), informing the operator about inconsistencies with the document template and supporting the biometric verification of the compliance of the photo and the person being identified.

4) The use of a dedicated mobile application and automatic verification allows users to carry out the verification process automatically based on the tools made available to the user. Remote verification mobile apps use artificial intelligence (AI) to analyze documents, recognize faces and compare data from the document with the person presenting it. AI algorithms are able to automatically check the authenticity of documents by analyzing their characteristics such as holograms, document structure, watermarks, as well as perform facial liveness detection to ensure that the user is actually present and is not using a recording or photo.

5) Identity card with an electronic layer and biometric confirmation – is an extension of the methods of automatic identity verification discussed above. As part of the method, the data of the identity document is downloaded directly using the antenna contained in the mobile phone (NFC) from the ID card or passport. This allows you to unambiguously confirm the use of an authentic document by the person being verified.

6) Sharing data from the mObywatel application – the mObywatel application also enables, in addition to using the mObywatel profile, sharing the data from stored mobile documents in local and remote processes. It not only contains identification data, but may also contain the holder's photo, authorizations and address information.

7) Qualified electronic signature - based on a qualified certificate. Such a qualified certificate identifies the person using the electronic signature in an unambiguous and reliable manner. The use of electronic signature in customer registration processes provides identification data of the person submitting the signed application or signing the contract, and documents undeniably the evidence related to the transaction being carried out. It is worth noting that the European Digital Identity Wallet, discussed later in the report, will enable all wallet holders to submit a qualified electronic signature.

There are already integrators on the Polish market who are delivering their services to customers – companies building on-boarding processes for their clients from various sectors – from banking, loan, insurance, through telecommunications and energy service providers to betting or lottery services. In addition to the above-mentioned methods, such integrators, or „eID hubs", also provide auxiliary tools that complement the remote on-boarding process, based on, for example, confirming selected data regarding the customer's bank account (AIS service) or other data necessary for the implementation of Know Your Customer (KYC) processes. An example of such a company is Authologic, which, in addition to local solutions, actively operates on various markets, providing comprehensive services for companies operating internationally.

In addition to those mentioned above, a new means of electronic identification should be indicated that will become widely used in 2026 – **the European Digital Identity Wallet.** This solution will enable the sharing of identification data at a high level of assurance. Apart from providing basic identity data, the wallet will allow you to store and share electronic confirmations of attributes, such as powers of attorney, permissions and certificates. In this respect, the implementation of identity confirmation using the wallet will enable both the reliable transfer of all identification data and the provision of additional data that may come from various reliable sources.

1.2. Legal regulations related to identity confirmation processes

The conditions for confirming identity are determined by many regulations at both the EU and national level. The most commonly used legal regulations in the field of identity proofing are listed below.

- **Regulations on administrative proceedings and digitalization of entities performing public tasks** – require identification of persons submitting applications and using public services. All public entities, when providing electronic services, use the national electronic identification system (login.gov.pl) and the means of identification made available there, i.e. a trusted profile, a personal profile, an mObywatel profile and bank electronic identification means connected to the national node.

- **The Act on Electronic Delivery** – requires the identification of both the sender and the addressee of registered correspondence – electronic registered delivery. In the field of electronic delivery, the services of the designated operator are based on the electronic identification means made available as part of the login.gov.pl. Qualified trust service providers use various methods to confirm the identity in order to register for electronic delivery services.

- **Anti-money laundering regulations** – impose on financial sector entities – in particular banks and insurers – requirements to confirm the identity of persons opening accounts, using payment instruments and life insurance. In Poland, specific requirements for remote identity confirmation in registering for financial services have been defined by the Chief Inspector of Financial Information, as well as by the Office of the Polish Financial Supervision Authority. Financial institutions successfully use remote and automatic ways of confirming the identity of users registering for financial services.

- **Telecommunications law** – requires registration of telephony customers and confirmation of their identity before providing services, in connection with countetracting terrorism. Telecommunications operators can rely on national and notified electronic identification means, use remote identity proofing methods as well as trust services, in particular electronic signatures.

- **The provisions of the eIDAS Regulation** – require confirmation of the identity of persons to whom qualified certificates for electronic signatures and seals are issued. The same applies to the qualified services of registered electronic delivery. Confirmation of identity required for the provision of qualified trust services is subject to specific quality conditions, must be carried out in accordance with European standards and periodically audited. Where electronic identification means are used, the regulations require the use of notified identification means with a high level of security and credibility.

Expert Insights

Michał Tabor
Member of the Management Board and Partner
Obserwatorium.biz

Digital identity of business

Effective electronic identification of business entities is the key to the efficient conduct of their business and the execution of transactions. Identifying companies also includes determining the identity of people acting on their behalf. These individuals, who have the appropriate powers of attorney, make declarations of will, which require their verification. Powers of attorney often are in the form of non-structured documents that require manual interpretation and prevent automated processing, slowing legal and administrative processes.

More effective and business-proven solutions are needed in this area. Electronic attestations of attributes as part of the European Digital Identity Wallet can eliminate these limitations. This solution will ensure a uniform form and interpretation of powers of attorney, enabling automatic data processing. Identifying persons acting on behalf of business entities has a chance to be simplified, and legal processes will become more efficient and consistent. A uniform format of electronic attestation of attributes will speed up the verification of powers of attorney, increase legal security, and reduce the risk of errors resulting from the misinterpretation of documents.

A European Digital Identity Wallet will complement the business needs of company identification for legal entities, enabling automatic interactions between entities based on pre-established rules. The company wallet solution, based on cloud technology, will allow for the automatic transfer of data and attributes of a legal entity without the need for interaction with a natural person. In the future, a company wallet combined with an electronic seal will enable declarations of intent on behalf of legal entities, automating business processes.

1.3 Examples of the use of remote identity confirmation in business

AUTOMATED APP-BASED IDENTITY CONFIRMATION PROCESS DURING ACCOUNT OPENING

Such processes, called „selfie accounts", are available in many banks – e.g. in Credit Agricole Polska Bank or ING Bank Śląski. At Nest Bank, the process of taking photos of documents with the option of a video call with a consultant has been implemented by IDENTT.

AUTOMATED IDENTITY CONFIRMATION PROCESS BASED ON THE mOBYWATEL PROFILE

Santander Bank Polska announced in 2024 that it had enabled the process of opening a personal account remotely using the mObywatel application. According to eIDAS 2.0, in the coming years the European Digital Identity Wallet will be a mandatory tool for remote identity confirmation and authentication in banking processes.

REMOTE SERVICE OF INSURANCE PRODUCTS

The mojeID KIR service allows you to create an account on insurance portals used to purchase and service insurance products. The leading example in this respect is the mojePZU portal.

IDENTITY VERIFICATION IN THE BNPL MARKET

The dynamically developing Buy Now, Pay Later (BNPL) market uses processes that improve identity verification, which allows for the issuance of an automated credit decision while reducing the risk of fraud. An example of an implementation is PayPO, which cooperates in this area with the service provided by IDENTT.

FULLY ON-LINE GAS CONTRACT USING VARIOUS METHODS

The process of concluding a gas supply contract at PGNiG's eBOK is 100% remote, and you can confirm your identity using one of the available methods, such as mObywatel, mojeID or e-ID / eDO App.

/EXAMPLE FROM ABROAD/ NEW TELECOMMUNICATIONS CONTRACTS WITH eID CARDS

Most telecommunications and utility providers in the Baltic States support national eID cards for user identification and the signing of new telecommunications contracts.

CONFIRMING IDENTITY AND AGE ON BETTING PLATFORMS

Due to restrictive legislation, the bookmaking sector requires the construction of onboarding processes with an emphasis on verifying the age of majority. An example of an implementation here is the introduction of Authologic tools.

CONFIRMING IDENTITY AND AGE ON THE LOTTO PLATFORM

The implementation of the mojeID KIR service in LOTTO made it possible to sell this well-known service online.

PARTNER'S USE-CASE

Jan Szajda
CEO and co-founder of IDENTT

The cooperation between IDENTT and Bank PEKAO S.A. has resulted in a modern KYC solution that streamlines and secures the account opening process. The system supports many verification methods, including a photograph of documents, the electronic layer of an ID card and integration with mObywatel. In 2023, 40% of all new accounts in Bank PEKAO were opened using IDENTT technology, which significantly reduced the cost of acquiring customers while minimizing the risk of identity fraud. Advanced biometric analysis enables an early detection of fraud attempts, increasing the overall level of security. The user-friendly solution offers customers the ability to choose their preferred verification method, which makes the process both efficient and secure.

1.4. The impact of eIDAS 2.0 and the Digital Identity Wallet on the future of the identity confirmation market

The 2014 eIDAS Regulation established a uniform standard for electronic identification and trust services in the EU, ensuring mutual recognition of notified identification systems and enabling citizens and businesses to use public and private online services throughout the EU.

The amendment to the eIDAS Regulation, which entered into force in May 2024, is a key element of the European Union's strategy to implement the **European Digital Identity Framework** to ensure harmonization of the rules and conditions for the use of trust services in the Member States. It will enable interoperability between national electronic identification schemes (eIDs) and trust services. The aim is to facilitate cross-border digital transactions in both the public and private sectors by making tools available and making them more interoperable.

The amendment focuses on the involvement of the private sector to a greater extent in the development and use of trust services, which will contribute to accelerating the adoption of digital identities and trust services. The main element of the implementation of the European Digital Identity Framework will be the implementation of the **European Digital Identity Wallet (EUDIW)**.

The European Digital Identity Wallet is a means that will enable its user to:

- store and share data about their identity;
- authenticate online and offline public and private services;
- collect attributes related to its identity and make them available to relying parties upon request;
- as well as submit qualified signatures and electronic seals

The wallet will be a tool that allows users to manage their digital identity and use it in various types of transactions, including business transactions. The basic implementation of the wallet will be a mobile phone application that will allow citizens to store and share digital versions of identity documents and other data, such as driving licenses, educational diplomas, medical data, bank credentials and insurance policies. The receipts provided by the wallet can be used to confirm identity and permissions remotely.

European digital identity wallets will support different types of identification documents, allowing users to use different forms of identification in a single, coherent digital identity solution. **The users of digital identity wallets will be natural persons, legal persons and natural persons representing natural persons or legal entities.**

Each Member State must make available and notify at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts, i.e. by the end of 2026. **Each such wallet will have to be recognised by every other Member State.** The European wallet will be issued by each European Union member state based on a solution it has built, but it will be based on a common digital identity standard that will be accepted in all EU member states. This will give users the opportunity to use a single, common digital identity solution throughout the European Union.

European identity wallets will be certified, among others, to meet the requirements for a high level of assurance. In addition, the wallet will comply with the General Data Protection Regulation (GDPR) and Member States are required to define technical and organisational measures to ensure a high level of protection of personal data.

The regulation by the end of 2027 **requires the recognition and acceptance of the digital identity wallet** by all entities obliged under the EU law, national law or contract to use Strong Customer Authentication. In addition, **all major online platforms will be required to introduce the possibility of logging in via wallets.**

PARTNER'S USE-CASE

Kai Wagner

Head of Products & Partners Procivis AG

The introduction of the European Digital Identity (EUDI) Wallet under eIDAS 2.0 is a groundbreaking step towards creating a unified digital identity ecosystem across Europe. It is set to empower businesses and citizens by enabling seamless access to trust services and fostering unprecedented identity enabled use cases.

The EUDI Wallet offers significant opportunities for both public sector and private sector entities. One of its most transformative aspects is the ability to issue and use interoperable attestations, such as identity documents, qualifications, licenses, or business authorizations that are recognized across all EU member states. This eliminates existing administrative burdens and opens the door to smoother, more efficient operations in sectors such as financial services, healthcare, hospitality, entertainment, logistics or education.

The Wallet's interoperability ensures that businesses that adopt these new solutions can work seamlessly across national borders, enabling secure and efficient identity verification and authentication with no vendor lock-in. The flexibility of the EUDI Wallet allows it to be integrated with existing platforms and workflows with minimal disruption.

By leveraging open standards and fostering a vendor-neutral approach, eIDAS 2.0 ensures that businesses can future-proof their digital identity strategies.

Ultimately, eIDAS 2.0 and the EUDI Wallet are poised to redefine trust and identity in Europe. They enable businesses to build greater operational efficiency while driving customer trust and satisfaction

1.5. Overview of remote identity proofing/ on-boarding service providers

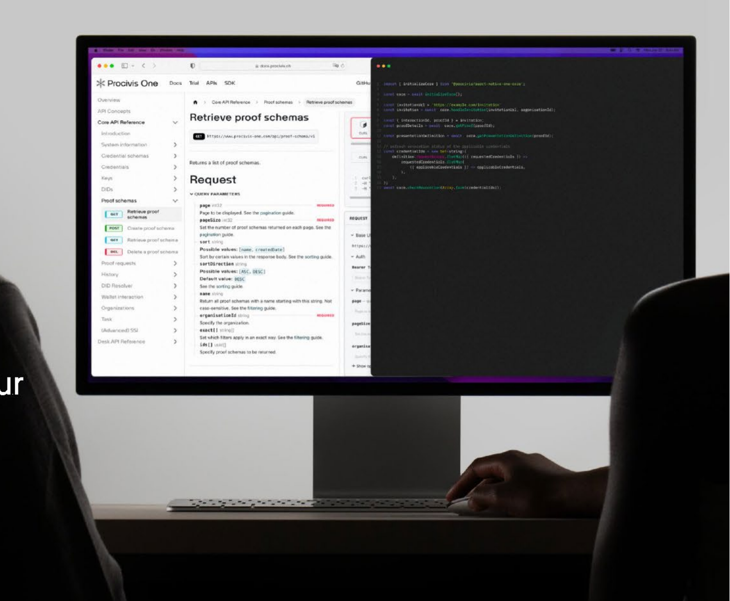
Subject	Solution name	Solution description
Authologic	Platforma Authologic	An end-to-end solution designed to streamline Know Your Customer (KYC) processes, providing both security and convenience for businesses and their users. The solution integrates various methods of identity confirmation into a single API. Using Authologic you can easily integrate with various vendors and include advanced user identification processes such as biometrics, liveness checks, electronic identity (eID) verification, document OCR, bank identification and many more. The solution allows you to reduce the KYC process time from 2-3 minutes to 10-30 seconds. It supports 200 countries and territories in 13 different languages.
IDENTT	Identt	IDENTT provides a system equipped with algorithms supporting the identity verification process. Support for various identity verification scenarios - based on document photos, the image of the person, the electronic layer of the identity document. Confirmation of the customer's identity can take place as part of the web application, mobile application, during a videochat conversation with a consultant or be integrated with an ATM. The solution is based on a database containing thousands of identity documents from over 194 countries.
KIR	mojeID	Identity means provision using electronic banking in commercial and public services. As part of the service offered on the company's website, customers are redirected to electronic banking, where they can securely and confidentially confirm their identity and agree to provide the required data. The entire process of confirming identity in electronic banking takes 20 seconds. MojeID is available to customers of 11 commercial banks and over 500 cooperative banks

Billon	**Billon's identity platform**	Billon's blockchain-based identity platform provides users with sovereign control over their digital identity, enabling seamless and secure interactions with service providers. Verified through a KYC (data provided by partners) process, actual identities are linked to digital ones, and personal information is stored off-chain in a secure identity registry. Once a sovereign identity is established, users have exclusive control over their cryptographic keys, allowing direct access to documents and services across the network without the involvement of third parties. Every interaction is uniquely encrypted and authenticated, reinforcing trust and data integrity in every transaction. Each identity verification transaction can be securely recorded on the blockchain, and the blockchain-based record offers a verifiable history of each identity verification.

The list includes only suppliers who are partners of the Trusted Economy Forum CommonSign 2024

Master eIDAS 2.0 with Procivis One

Procivis One is a flexible, end-to-end software solution for the eIDAS 2.0 ecosystem, seamlessly connecting your business case and current implementations to the new European Digital Identity Wallet framework.



AVAILABLE AS TWO LICENSE MODELS:

Procivis One Open Source

Procivis One Enterprise

API SDK WEB

01. Procivis One Issuer

Complete Provisioning & Lifecycle Solution for the EUDI Wallet Ecosystem to issue PID, QEAA, PuB-EAA or EAA into any EUDI Wallet.

02. Procivis One Verifier

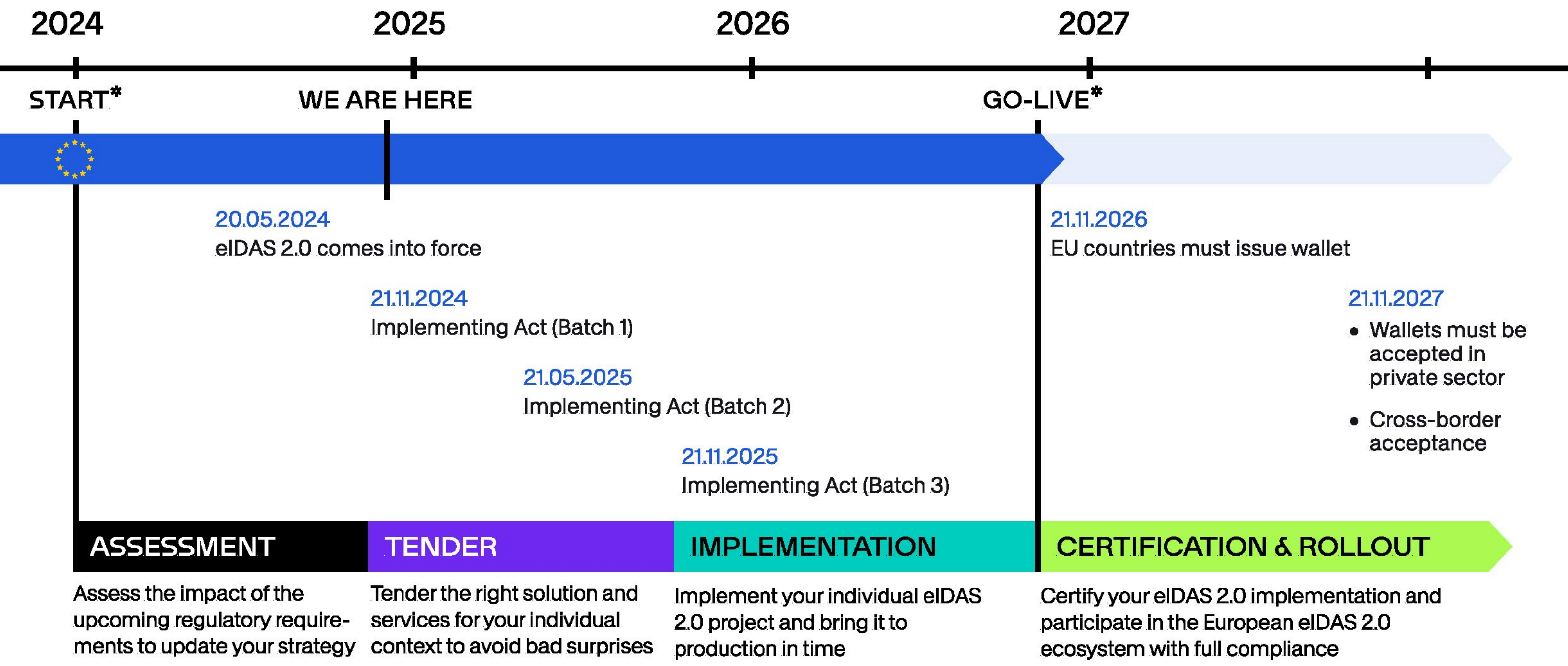
Complete Relying Party Solution for the EUDI Wallet Ecosystem to verify PID, QEAA, PuB-EAA or EAA from any EUDI Wallet.

03. Procivis One Wallet

Complete EUDI Wallet SDK for free standing or embedded EUDI Wallet Apps that can be adapted to your member state needs.

Keep the eIDAS 2.0 Timeline in Mind

The eIDAS 2.0 regulation could impact your business in multiple ways. Check the timeline below for an overview, and contact Procivis for a detailed compliance assessment and migration pathway.



20.05.2024
eIDAS 2.0 comes into force

21.11.2024
Implementing Act (Batch 1)

21.05.2025
Implementing Act (Batch 2)

21.11.2025
Implementing Act (Batch 3)

21.11.2026
EU countries must issue wallet

21.11.2027
- Wallets must be accepted in private sector
- Cross-border acceptance

ASSESSMENT
Assess the impact of the upcoming regulatory requirements to update your strategy

TENDER
Tender the right solution and services for your individual context to avoid bad surprises

IMPLEMENTATION
Implement your individual eIDAS 2.0 project and bring it to production in time

CERTIFICATION & ROLLOUT
Certify your eIDAS 2.0 implementation and participate in the European eIDAS 2.0 ecosystem with full compliance

🟦 EU timeline ▨ Recommended development phases * Earliest & latest dates to start or be ready

Procivis
AN ORELL FÜSSLI COMPANY

info@procivis.ch
www.procivis.ch
+41 44 523 65 35

Dietzingerstrasse 3
8003 Zurich
Switzerland

Zimmermanngasse 8
1090 Vienna
Austria

ATTESTA ISO 9001 ZERTIFIZIERT

ATTESTA ISO 27001 ZERTIFIZIERT

IDENTT®

We assure you!

By the nature of biometrics

IDENTT is a leading provider of AI-based solutions for **automatic identity document verification** and **biometric facial recognition**.

We offer enhanced security by **minimizing identity fraud** and **reducing client acquisition costs**.

These services help businesses streamline remote or onsite customer onboarding and meet legal compliance standards.

- Identity verification
- Automated and remote Customer onboarding
- Document OCR
- E-contracting
- Frauds Detection
- Age verification

2. Qualified electronic signatures

Qualified electronic signatures are a form of electronic signatures with the highest level of security and trust, regulated in the European Union by the eIDAS regulation (Regulation of the European Parliament and of the Council of the EU No. 910/2014). They are **legally equivalent to a handwritten signature,** which means that a document signed with a qualified electronic signature is treated as if it had been signed by hand.

A qualified electronic signature is a tool that enables **a declaration of intent - signing documents remotely,** but with the highest level of security and legal compliance. It is crucial for individuals and organisations that need a legally binding signature that is accepted in all EU countries. It allows you to safely conduct operations and conclude contracts with full confidence in their authenticity and integrity.

Electronic signatures in accordance with the eIDAS Regulation are the result of the activities of trust service providers, which, as supervised entities, provide solutions based on compliance with the requirements of regulations and trust service policies. A qualified electronic signature carries presumptions of both credibility and integrity of the document and that the person indicated in the certificate has signed the document or statement.

2.1. Qualified electronic signature as a tool for remote declaration of intent in business processes

A declaration of intent is an expression of a decision made by a natural person or a person acting on behalf of a legal entity, which is aimed at producing specific legal effects. It functions as a formal confirmation of undertakings or concluding a contract.

In Polish law, the principle of freedom of form of declaration of will applies. According to Article 60 of the Civil Code: „Subject to the exceptions provided for in the Act, the will of a person performing a legal act may be expressed by any conduct of that person which reveals his will in a sufficient manner, including by revealing this will in electronic form (declaration of will)."

With the entry into force of the eIDAS Regulation, the Polish legislator introduced Article 78 to the Civil Code (amendment of 8 September 2016), which aims to unify the rules for the use of the electronic form of legal transactions. As a result of the above changes, the electronic form has been clearly distinguished in the Polish legal system **as an autonomous form of legal transactions**. Previously, the distinction of the electronic form was a contentious issue since it was treated as a variation of the written form.

The amendment to the Civil Code also introduced a new special form of performing legal acts – **the documentary form**, for which it is sufficient to submit a declaration of intent in the form of a document, in a way that allows the person making the declaration to be determined. A document is understood here as a carrier of information that can be read by other people. Therefore, it does not have to be a declaration of intent in the form of an electronic document. Video, audio or email recording is also acceptable. The document form is not automatically an electronic signature and does not carry legal presumptions resulting from the use of electronic signatures. Since the law does not specify the conditions of security and the use of the documentary form, the entire burden of securing it and proving related to its use is on the complainant. The party taking evidence in terms of the documentary form should confirm its integrity and connection with the person making the statement. Therefore, the documentary form should be used only where the risk associated with the value of the transaction is low. Electronic signatures, in particular advanced electronic signatures and qualified electronic signatures, guarantee the integrity of the document and the relationship with the signer.

Currently, we have several options for making a declaration of will. It can be submitted:

- verbally,
- in writing:
  - in an ordinary written form,
  - in writing with a certain date, i.e. officially certified,
  - in writing with a notarized signature,
- in the form of a notarial deed,
- in documentary form,
- implicitly (through non-linguistic behaviour, but one that reveals our will in a way that is sufficiently understandable to the recipient),
- **in electronic form.**

In order to maintain the electronic form of a legal transaction, two conditions must be met:

1.
submission of a declaration of will in an electronic form

2
providing it with a qualified electronic signature

A declaration of intent made in electronic form is equivalent to a declaration of will made in writing. In any case where a handwritten signature is required, it can be effectively replaced by a qualified electronic signature. **Therefore, if the provisions of law require the written form to be valid for a legal transaction, it may be replaced by the electronic form.**

Currently, thanks to **the legal equalization of the written form with the electronic form,** when signing documents related to the company's operations, including contracts for the validity of which the notarial form of a legal act has not been legally or contractually reserved, the parties can use handwritten signatures or qualified electronic signatures. What is more, it is permissible for one party to a legal transaction to submit a statement in writing and the other in electronic form.

The security of a qualified electronic signature is guaranteed by trust service providers, who are subject to strict security requirements and supervision carried out by the state

In order to maintain the electronic form, it is not required to submit a qualified electronic signature based on a certificate issued in Poland, the signatory may use a qualified electronic signature based on a certificate issued as qualified in any European Union member state.

Qualified electronic signature providers are entered on European trust lists and are subject to strict organizational, capital, cybersecurity and quality of service requirements. The certificate can be issued on-site (in the branches of these institutions, their partner points or through a network of representatives), and more and more often also on-line with the use of specific remote identity confirmation tools.

In addition, there are **signature platforms** on the market which most often provide mechanisms for electronic circulation of documents and handling the process of their signing using various types of electronic signatures, including qualified signatures. In Poland, examples of such platforms are Autenti, Pergamin or Umownik.

2.2. Legal regulations related to electronic signatures

eIDAS sets standards and rules for electronic identification, authentication and trust services such as electronic signatures, seals, digital certificates, electronic delivery services and timestamping services.

The regulation, which has already been mentioned many times in this report, implements the process of digitalization offering a framework for the use and recognition of electronic signatures and seals that perform functions analogous to traditional paper equivalents. In particular, qualified electronic signatures have the power to replace handwritten signatures, and electronic seals are used to confirm the authenticity and integrity of electronic documents.

Advanced and qualified electronic signatures defined in eIDAS are special categories of electronic signatures that meet additional requirements, such as **unique assignment to the signer, the ability to uniquely verify the identity** of the signer and proof of signature and document integrity. Qualified electronic signatures, based on a qualified certificate and a qualified device for creating signatures, are legally equivalent to handwritten signatures. Qualified electronic signature creation devices provide a secure and signer-controlled signature creation environment. Currently, cryptographic cards and remotely available data management services for creating electronic signatures are used as qualified devices for creating signatures. The most important security feature of signature creation devices is the signer's exclusive control over the use of the signature device. The law prohibits the sharing of one electronic signature device by many people or its use by a third party.

Qualified electronic signature certificates are issued by trust service providers after unambiguous verification of the signer's identity. These certificates are open and attached to each signed document, enabling verification of the submitted electronic signatures.

Qualified electronic signatures are recognized throughout the EU. A qualified electronic signature based on a qualified certificate issued in one Member State is considered a qualified electronic signature in all other EU Member States. This requirement of EU regulations imposes on entities verifying electronic signatures the obligation to use solutions that allow for the recognition of not only domestic but also foreign electronic signatures in recognizable formats.

The eIDAS regulation, amended in 2024, introduces many changes in both the area of identification and trust services. One of the most important changes is the introduction of European Digital Identity Wallets to facilitate access to a variety of digital services and improve the protection of users' privacy. In accordance with the provisions of the regulation, **individual users**, i.e. citizens in each member state of the European Union, will be offered by default and without unnecessary administrative procedures solutions including qualified electronic signatures (QES) available through (EUDIW), which they will be able to use **free of charge as part of the so-called non-professional use.**

It is worth noting that the revised version of eIDAS also includes provisions suggesting that Member States should be able to establish measures to prevent the free use of qualified electronic signatures by individuals for professional purposes, while ensuring that any such measures are proportionate to the identified risks and justified

2.3. Examples of the use of a qualified electronic signature in business

DIGITIZATION OF DOCUMENT FLOW IN A LEASING COMPANY

Lessors such as BNP Paribas Lease Group and Santander Leasing provide the possibility of remote signing of e-documents, e.g. leasing agreements, with a qualified electronic signature. The provider is Asseco Data Systems, which offers SimplySign and SIGNER API systems that can be integrated with the company document workflow systems.

ISSUANCE OF QUALIFIED ELECTRONIC SIGNATURES BASED ON BANK IDENTITY

More and more banks in Poland enable the issuance of qualified electronic signatures to their customers on the basis of identity confirmation using bank means of identification. The National Clearing House allows the issuance of a signature certificate, the so-called mSzafir min. customers of PKO BP or Bank Millennium. Asseco Data Systems offers a similar solution – the SimplySign product – to customers of Santander Bank Polska.

PARTNER'S USE-CASE

Artur Miękina

Director of the Project Sales and E-Business Development Department
Asseco Data Systems

The implementation at ING Bank Śląski is an example of the cooperation, willingness and commitment of the parties to digitize HR processes. The innovative concept of utilizing the single-use qualified signature as an optimal, reliable and safe solution has been an integral part of this complex project. Thanks to the comprehensive approach, HR processes have become more effective and ecological, while at the same time eliminating paper documents. We see great potential for the use of a single-use qualified signature, not only in the area of HR, but also in business.

PARTNER'S USE-CASE

Bogumiła Cebelińska-Woźniak

Product Director Billon Group

Billon's blockchain-based remote document management and contracting platform is an advanced solution that integrates e-signatures, e-deliveries and digital identity management by offering various online verification methods. Blockchain technology provides an immutable, transparent record of each transaction, which enables secure verification and a full audit trail of business processes. The platform complies with eIDAS regulations, GDPR and durable medium requirements, meeting the highest security and data protection standards. Currently, it is implemented in the financial sector as part of the BIK platform for banking and insurance and in the energy sector at the leading energy supplier Tauron. Other implementations include the education and green energy sectors. Our solution has also undergone extensive testing as part of the European Blockchain Services Infrastructure (EBSI) initiative for a cross-border data and document exchange process. Thanks to its modular architecture, the platform flexibly adapts to the individual needs of customers, offering complete digital support for documentation and contracts.

PARTNER’S USE-CASE

Andrea Sassetti
CEO
Aruba PEC

An Italian Financial Services company tied to the Stock Exchange has successfully implemented multiple trust services to automate the management of the Register of Members for its clients. This essential document identifies valid members and establishes quorum for meetings, ensuring the legitimacy of intervention and voting. Leveraging Aruba PEC S.p.A.’s Certified Platform, this company produces the Shareholders’ Register in PDF format and streamlines the process. Upon loading the document, an automated workflow initiates, facilitating e-signatures by both the financial services company’s operator and the client company representative. The signed document is then securely sent via a qualified e-Delivery service and stored in qualified e-archiving facility ensuring compliance with legal requirements. This integration of automated e-signature and e-delivery services not only enhances the security and efficiency of document management but also guarantees legal validity, showcasing an exemplary model of trust services in action. A combination of trust services streamlines operations while adhering to regulatory obligations seamlessly.

PARTNER'S USE-CASE

Edgars Stafeckis

CEO & Co-founder TrustLynx

Trustlynx's Embedded Trust platform was launched at a time when trust services such as electronic signatures and electronic seals were primarily used in public services and only optionally in the private sector. The true importance of trust service adoption became apparent during the COVID-19 pandemic, when the ability to do business, provide services, and complete transactions entirely remotely was made possible by digital identities, electronic signatures, electronic seals, etc. The use of trust services has increased exponentially and this trend continues. Digital identities, electronic signatures and electronic seals have become an indispensable element of modern business.

The Trustlynx platform offers secure, flexible and efficient tools to enrich your organization's systems with the right trust services, including support for digital identities and their attributes, electronic signatures and their collection, electronic seals and their validation. In the digital world, the priority is a seamless user experience, information security, and data protection – it's not only a necessity, but also a competitive advantage. Trustlynx has developed trust service integration and automation technology to simplify the development of business processes and digital products, offering end-to-end solutions to modern businesses.

Now that electronic signatures are legally equivalent to handwritten signatures, Trustlynx is a trusted partner, providing flexible and secure solutions. The Embedded Trust platform enables businesses to simplify the user journey and data flow without compromising security or compliance, enabling them to keep up with the pace of digital transformation.

2.4 Qualified electronic signature compared to other types of signatures on the Polish market and in the perspective of the implementation of eIDAS 2.0

The eIDAS Regulation defines two types of signatures other than qualified ones: an advanced electronic signature and an simple electronic signature. In the case of electronic signatures other than the qualified, each trust service provider determines the conditions of its security and the scope of the service provided.

These two other types of signatures, although they do not meet the written form and do not replace a handwritten signature, are successfully used in the Polish digital space. They are also used in various situations. Regardless of the type of electronic signature, they cannot be denied legal effect or admissibility as evidence in court proceedings solely because the signature is in electronic form or does not meet the requirements for qualified electronic signatures. The main differences between individual electronic signatures are presented in the table below.

Types of electronic signatures:

Function	Qualified electronic signature	Advanced electronic signature	Ordinary electronic signature
Legal force	Recognized in all European Union countries in a uniform manner	Recognised locally or in business relations, it provides evidential value at the European level	Recognized locally or in business relations
Qualified electronic signature certificate	Required	Optional	-
Issuer of a qualified electronic signature certificate	EU or Norwegian Qualified Trust Service Provider	Qualified or non-qualified trust service provider	-
Qualified signature creation device	Required	-	-
Can be submitted remotely	Yes	Yes	Yes
Proof of signer identity	Required by law with a high level of assurance; can be local or remote	Required, but the level of certainty may be limited	-
Accepted in public tenders	Yes	No	No

The above-mentioned non-qualified electronic signatures function in Polish circulation under their own names, such as trusted signature and personal signature.

Comparison of qualified signatures and government solutions (personal and trusted signatures):

	Qualified signature	Trusted signature based on the Trusted Profile	Personal signature based on an electronic ID card
Onboarding	Application for a signature submitted online + confirmation of identity onsite or remotely (video verification, eID, other qualified signature)	Application for a signature submitted online + onsite or remote identity confirmation (video verification, eID, other qualified signature, ID card with an electronic layer + NFC)	It depends on the procedure for obtaining an ID card (currently only stationary)
Functionality, access channels	Application for a signature submitted online + confirmation of identity onsite or remotely (video verification, eID, other qualified signature)	Possibility for public entities to send (to the appropriate API) a document for signature and return the signed document / Web browser	To use a personal signature, you need to have an NFC reader for your e-ID (or a smartphone with an NFC reader) and install the appropriate software on your device (E-ID personal signature or eDO App)
Validation of signed documents/ interoperability	Desktop tools provided by signature providers, qualified validation services, DSS on the European Commission's website, Obywatel.gov.pl	On the obywatel.gov.pl website, the e-ID application, some applications for the verification of qualified signatures/lack of interoperability outside of PL in the field of creating and submitting as well as verifying signatures	The e-ID application and some applications for the verification of qualified signatures/lack of interoperability outside of Poland in the field of creating and putting a signature
Effects of use, legal force	A qualified signature replaces traditional paper documentation (automatically equivalent to a handwritten signature)	Data in electronic form bearing a trusted signature are equivalent in terms of legal effects to a document bearing a handwritten signature, unless separate provisions state otherwise	An effect equivalent to a handwritten signature is the personal signature of the data in relation to an entity other than a public entity, if both parties agree to it
Use cases, reach	can sign with a trusted signature and sign B2B and B2C contracts	Dealing with official matters on dedicated platforms (ePUAP, obywatel.gov.pl, PUE ZUS, praca.gov.pl). Lack of acceptance coverage in the business area	It has the same functionality as the Trusted Signature and is used to communicate with Polish administration systems. In B2A relations

The use of qualified signatures gives the widest possibility of obtaining approval of a document signed with such a signature. A trusted signature is not recognized as a signature outside Poland, while a personal signature will be recognized, but trust in it will be limited. A trusted signature is not accepted in business, while a personal signature can be used in commercial services with the consent of both parties. **A qualified signature provides the most possibilities for use in both the public and private-commercial sectors.** Due to the security guarantees offered, a qualified electronic signature is increasingly used instead of other weaker signatures.

Despite many unresolved technical issues, it can already be assumed that the **wide adoption of the wallet among citizens of the Member States will significantly change the number of interactions in which a qualified electronic signature can be used.** After the wallets become popular, every citizen of a member state will be able to sign any contract, including, for example, an employment contract with full legal force using an easily available qualified electronic signature. Potentially digitization on a mass scale will be possible for processes that have so far been reserved only for implementation in direct physical contact between the customer and the institution or, in selected cases, with other models, such as a physical signature in the presence of a courier, or in which tools that are insufficient from the security point of view, such as the document method, were used.

2.5. Overview of electronic signature providers and services

Subject	Solution name	Solution description
Asseco Data Systems	SimplySign (Certum by Asseco)	SimplySign is a mobile electronic signature that does not require a physical reader or a certified card. Sign from your smartphone, tablet, laptop, PC, or Mac. Compliance with key services and platforms such as e-declarations, ePUAP, ZUS and eKRS. Compatible with CertumSign - a platform for signing e-documents via a browser. The signature can be seamlessly integrated with any document or transaction workflow system or any electronic banking system through the SimplySign API (a solution that allows you to use the qualified SimlpySign e-signature directly in the document workflow system). Compatible with the SignHUB solution that allows people outside the organization to sign documents, even if they do not have their own e-signature.

Subject	Solution name	Solution description
Aruba S.p.A	Firma digitale remota	A remote digital signature includes a timestamp that allows you to associate a specific date and time with the documents you sign and extend their legal validity to 30 years. With the dedicated Aruba OTP app for remote digital signature, you can generate a one-time two-factor OTP authentication code and sign directly from your smartphone, without other devices. The solution is compatible with Aruba Webmail and PEC Webmail. As a result you can sign documents directly in your email inbox without having to install any signing software or application.
Namirial Group	Namirial Digital Signature	Designed to manage files and documents directly from your smartphone. Identification via video identification session via webcam with a Namirial operator is included in the price. Full eIDAS compliance Multi-factor authentication for maximum security. Compatible with the eSignAnyWhere signature platform, which can be integrated with popular tools such as Microsoft Office 365, Salesforce or SharePoint and deployed as a cloud service or on-premises.
KIR	mSzafir	The mSzafir mobile qualified electronic signature allows you to sign documents on any device and allows you to generate one--time certificates and certificates valid for 1 or 2 years with a selected limit of signatures. The user's identity is verified using the mojeID service (using electronic banking), a qualified certificate or in person at a KIR branch. The solution offers the possibility of signing up to 20 documents at the same time.
SIGNIUS S.A.	SIGNIUS Professional - a platform for remote signing of documents with qualified and advanced signatures	The platform allows documents to be signed remotely and instantly online with an advanced and qualified signature by multiple people. A qualified signature (Eurocert certificate) is issued on the basis of remote identity verification carried out in the form of video verification or independently through the Nect Selfie application.

The list includes only suppliers who are partners of the Trusted Economy Forum CommonSign 2024

ARUBA FOSTERS TRUST AND TRANSPARENCY WITHIN BOTH THE EUROPEAN AND GLOBAL DIGITAL ECONOMIES

Aruba.it

Namirial

Making Simplicity Meeting Compliance

Harnessing Namirial Intelligent Trust Services for, among other things …

SALES

- Purchase agreements
- Account opening
- Financing contracts (loan / leasing)
- Consultation records
- Direct debit mandates (SEPA)
- Leases / rental agreements
- Confidentiality agreements (NDA)
- Reseller / referral agreements

HUMAN RESSOURCES

- Working contracts
- Confidentiality agreements (NDA)
- Employee policies
- Consent declarations
- Permits
- Expense processing
- Bonus agreements

SERVICE / SUPPORT

- Support agreements
- Maintenance contracts
- Damage reports
- Repair orders
- Amendments
- Acceptance protocols

PROCUREMENT

- Supplier contracts
- Service contracts
- Consulting agreements
- Requirements acceptance
- Orders
- Amendments
- Payment releases

LEGAL

- License agreements
- Consent declarations (GDPR)
- Agreement amendments
- Distribution agreements
- Facility management contracts
- Memoranda of understanding
- Authorities

QUALITY MANAGEMENT

- Order processing
- Standard operating procedures (SOP)
- Test protocols
- Loan documents
- Proofs of waste disposal

Talk to us about your use cases at Trusted Economy Forum CommonSign 2024

Anthony Skarlatos
Key Account Manager
Namirial

✉ a.skarlatos@external.namirial.com
☎ +30 694 4316 302
in linkedin.com/in/antonyskarlatos/

Jörg Lenz
Head of Marketing & Communication
Namirial

✉ j.lenz@namirial.com
☎ +49 174 2409 299
in linkedin.com/in/joerglenz

Namirial – Pan-European Qualified Trust Service Provider according to EU Regulations eIDAS 910/2014 + 2024/1183

TRUST LYNX

The trustworthy signature!

E-signatures and e-seals compliant with Polish and EU regulations.

TrustLynx is an innovative, secure, and easy-to-use solution for integrating, automating, and digitizing business processes.

- Integrations with any CRM, HR system, or other business applications
- Compliant with eIDAS
- User-friendly interface and seamless signing process
- Work automation and time savings
- Environmental protection

trustlynx.com sales@trustlynx.com

billon

BILLON

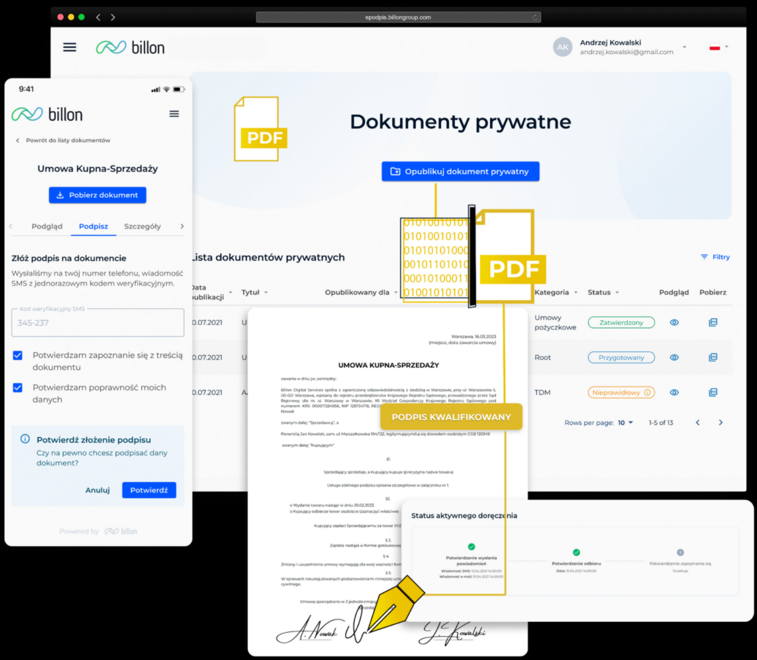
Billon is a technology company that has developed its own ultra-efficient, data-centric blockchain protocol. The platform fully supports the growth of Web 3.0 and holds a world record for energy efficiency. It enables the seamless processing of data, documents, identity, tokens, and money within a unified infrastructure, driving improvements in processes, security, and automation. Billon's solution represents a revolution in data management and has been tested and verified by globally recognized companies.

BILLON UNIFIED BLOCKCHAIN

BILLON UNIFIED BLOCKCHAIN

Billon Unified Blockchain is a modern blockchain platform that combines a durable medium of information with the secure exchange of data and documents on-chain, compliant with national and European regulations, including eIDAS and GDPR. It enables remote declarations of intent, contract signing, and the use of advanced e-signatures while supporting digital identity management and electronic identification. Through its active delivery feature, the platform confirms the delivery and receipt of documents linked to a verified identity, ensuring data immutability, complete auditability, and operational security in the Web 3.0 era.

- Durable medium of information for both public and private documents
- Digital signatures including SES, AES, QES
- Flexible authentication methods and role management
- Digital identity as the foundation for sovereign identity (SSI)
- Active delivery - undeniable evidence of cryptographically secured document delivery and receipt



epodpis.billongroup.com

billon

Andrzej Kowalski
andrzej.kowalski@gmail.com

Dokumenty prywatne

Opublikuj dokument prywatny

Lista dokumentów prywatnych

Filtry

Data publikacji	Tytuł	Opublikowany dla	Kategoria	Status	Podgląd	Pobierz
0.07.2021	U		Umowy pożyczkowe	Zatwierdzony		
0.07.2021	U		Root	Przygotowany		
0.07.2021	A		TDM	Nieprawidłowy ⓘ		

Rows per page: 10 ▾ 1-5 of 13 ‹ ›

9:41

billon

‹ Powrót do listy dokumentów

Umowa Kupna-Sprzedaży

Pobierz dokument

Podgląd | Podpisz | Szczegóły

Złóż podpis na dokumencie

Wysłaliśmy na twój numer telefonu, wiadomość SMS z jednorazowym kodem weryfikacyjnym.

Kod weryfikacyjny SMS
345-237

☑ Potwierdzam zapoznanie się z treścią dokumentu

☑ Potwierdzam poprawność moich danych

ⓘ Potwierdź złożenie podpisu
Czy na pewno chcesz podpisać dany dokument?

Anuluj | Potwierdź

Powered by billon

Warszawa, 16.03.2023
(miejsce, data zawarcia umowy)

UMOWA KUPNA-SPRZEDAŻY

zawarta w dniu jw. pomiędzy:

Billon Digital Services spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, przy ul. Warszawska 5, 00-021 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 000017284956, NIP 128734718, REG[illegible]
Nowak

zwanym dalej: "Sprzedawcą", a

Panem/ią Jan Kowalski, zam. ul. Marszałkowska 104/122, legitymującym/cą się dowodem osobistym CGB 120349

zwanym dalej: "Kupującym"

§1.

Sprzedający sprzedaje, a Kupujący kupuje (precyzyjna nazwa towaru)

Usługa zdalnego podpisu opisana szczegółowo w załączniku nr 1.

§2.

o Wydanie towaru nastąpi w dniu 20.02.2023.
o Kupujący odbierze towar osobiście (zaznaczyć właściwe)

Kupujący zapłaci Sprzedającemu za towar XYZ

§ 3.
Zapłata nastąpi w formie gotówkowej

§ 4.
Zmiany i uzupełnienia umowy wymagają dla swej ważności form

§ 5.
W sprawach nieuregulowanych postanowieniami niniejszej um cywilnego.

Umowę sporządzono w 2 jednobrzmiący

A. Nowak J. Kowalski

PODPIS KWALIFIKOWANY

Status aktywnego doręczenia

Potwierdzenie wysłania powiadomień
Wiadomość SMS: 15.04.2021 14:00:00
Wiadomość e-mail: 15.04.2021 14:00:00

Potwierdzenie odbioru
Data: 15.04.2021 14:00:00

Potwierdzenie zapoznania się
Oczekuje

CONTACT

General
contact@billongroup.com

Chief Commercial Officer
jacek.figula@billongroup.com

TDM Product Director
bogumila.cebelinska@billongroup.com

www.billongroup.com

3. Qualified electronic seals

An electronic seal is a tool that provides evidence of the integrity and authenticity of the origin of documents sealed with it. An electronic seal can only be used by legal persons – for example, companies, offices and social organizations. Its most common way of using is to authorize official company correspondence, legal documents, diplomas, ID cards and confirmation of services which therefore do not have to be issued in paper and do not require human interaction.

By definition, according to the eIDAS Regulation, „Electronic Seal" means **data in electronic form** added to or logically linked to other data in electronic form **to ensure the authenticity of origin and the integrity of the related data**

3.1. Qualified electronic seals as tools for legal entities in business processes

The most characteristic feature of an electronic seal (including a qualified seal, of course) is that **it can be used by legal persons**, i.e. companies, organizations or institutions.

It is, in addition to the electronic signature, created as a result of trust services, which are to enable the implementation of confirmation of the origin and integrity of a document that is electronically „sealed". A qualified electronic seal is very similar to a qualified electronic signature in terms of its legal and technical structure. However, it is not the equivalent of an electronic signature of a legal person.

In the current legal status in Poland, a qualified electronic seal does not allow for the submission of a declaration of intent in an electronic form and does not replace a handwritten signature.

A qualified electronic seal can therefore be used wherever it is necessary to ensure the guarantee of data integrity, where it is necessary to increase the security of the archiving process and digitization of paper documents (thanks to this service, we can be sure that both versions are compatible). It is important that a qualified electronic seal can also be used to secure internal company documents. Thanks to this, we will not only confirm the authenticity of documents and the integrity of data, but also protect them from falsification.

The possibilities of using a qualified electronic seal are available in many areas, especially such as finance, the insurance sector, public administration, logistics and medical services.

The use of an electronic seal enables the introduction of automated and secure B2B and B2C electronic communication. It also allows for long-term protection of stored documents. Qualified electronic seals can be used both in documents sent to contractors and in the case of documents within the company, such as:

- **Serial documents such as messages,** account statements, insurance policies, etc.;
- **Institutional notices, such as confirmations,** certificates and diplomas;
- **Patients' medical records**, including discharge reports and medical records;
- **Legal acts** (e.g. laws, regulations);
- **Enterprise documents,** regulations, organizational documents;
- **Contracts and commercial proposals**;
- **E-invoices, receipts, order receipts and delivery documents**
- **Mailroom service** – outgoing and incoming documents,
- **Securing employee files** – securing files, changing the form.

The use of seals makes it easier to automate processes in DMS or ERP systems and improve many business activities in accounting, sales, customer service and HR departments. It allows for cost reduction and saving of time when handling documents and makes it possible to mark many documents simultaneously. It reduces the administrative burden by eliminating paper-based office activities. It increases the credibility of transactions. It is used for the secure exchange of documents with internal and external entities. It allows you to use the full range of digital services that have already been implemented. Finally, it strengthens the professional image of the company using innovative solutions.

An important example of the use of an electronic seal is the possibility of using it in administrative proceedings as a substitute for an electronic signature. In accordance with the provisions of the Code of Administrative Procedure, public administration bodies have the possibility to issue letters in electronic form using ICT systems with a qualified electronic seal. An electronic seal, as an advanced tool for confirming the identity of the authority issuing the document, guarantees that the letter comes from the competent authority and its content has not been changed. On the other hand, such a document contains information about the person who drafted the letter in the text part. Documents with a qualified electronic seal do not have to contain an electronic signature.

The electronic seal is also successfully used to confirm the receipt of letters in public administration systems, where the official confirmation of receipt is carried out automatically at the time of receipt of the letter to the office and provided with the electronic seal of the office. In addition, in all registered electronic delivery services the proofs of sending, sharing and issuing parcels are provided with an electronic seal.

3.2. Use of the electronic seal in specific sectors

DIGITALIZATION OF TELECOMMUNICATION SERVICE SALES PROCESSES

Polsat Plus Group, the largest media and telecommunications group in Central and Eastern Europe, has built new digital sales processes thanks to Asseco, Xtension and Samsung, which support the implementation of paperless strategies in enterprises. The reason for the change was the company's strategy and the reduction of costs, handling time and maintenance of archiving related to paper documents.
The new customer service process in POS and sales takes place fully electronically using a tablet with hardware security software. The documents signed on it are provided with a qualified electronic seal and a qualified electronic time stamp in accordance with the European eIDAS regulation.

ONLINE SEALING OF BANK DOCUMENTS

The electronic seal enables the sealing of mass correspondence directed to bank clients or automatically generated documents, such as transaction transfer confirmations. It also meets the requirements of the so-called durable media, primarily because the service provider acts as a trusted third party in the bank-client relationship.

PARTNER'S USE CASE

Antony Skarlatos
Key Account Manager
Namirial

Transforming Business Operations with Trusted Digital Solutions

As digital transformation reshapes the modern business landscape, integrating e-signatures, e-seals, and eID solutions is crucial for businesses aiming to stay competitive. Namirial's innovative digital tools provide organizations with the foundation to streamline operations, secure sensitive data, and navigate complex regulatory requirements with confidence.

With years of experience supporting Polish businesses in critical sectors such as finance, healthcare, and telecommunications, Namirial offers tailored solutions that address both national and European compliance needs. Through strategic partnerships with experienced Polish companies, we ensure businesses meet local demands while tackling broader European regulatory challenges.

Our advanced solutions, including Self ID and Video ID, leverage AI-driven face-matching technology to simplify and accelerate KYC and AML processes, ensuring fast, secure, and virtually fraud-proof identity verification. Additionally, Namirial's e-signatures and e-seals are key to simplifying document management and contract execution, ensuring legally valid agreements and supporting cross-border interoperability—vital for businesses expanding globally.

Namirial's API-driven end-to-end platform integrates seamlessly into existing IT infrastructures, driving operational efficiency, reducing costs, and fostering a transition to a paperless future. By adopting Namirial's digital solutions, Polish businesses unlock new opportunities for growth and innovation while ensuring compliance with evolving regulatory standards.

3.3. Overview of electronic seal suppliers

Subject	Solution name	Solution description
Asseco Data Systems	Certum qualified electronic seal	The qualified Certum electronic seal is available in two variants: saved on a card inserted into the reader and in the SimplySign mobile application. The seal can be seamlessly integrated into any document/transaction workflow system or any electronic banking system using the SimplySign API, which is a simple, fast and efficient solution, especially for the enterprise sector. It can be used in the company's external and internal circulation to authenticate and maintain the integrity of documents (invoices, employee documentation, reports, etc.)
Aruba S.p.A	Qualified seal certificate for smart cards or hardware security modules (HSMs)	Ideal for public authorities as it allows you to issue certificates online, saving resources in terms of both cost and time. The solution is perfectly integrated with all digital signature solutions. Possible application integration via Aruba virtual infrastructure and APIs for all remote digital signatures.
Namirial Group	Namirial Electronic Seal	The Namirial electronic seal can be easily applied to all kinds of documents, such as invoices, official notices, quotations or other documents that require a commitment from the company. The solution certifies any file type (text, audio, and video files). Available with a shelf life of one or six years. The solution is available with dedicated FirmaCerta software. It works without additional devices and without any authorization codes to enter.
KIR	Sapphire Electronic Seal	The Szafir electronic seal identifies the company, ensures data integrity, authenticates the sender and meets all the legal requirements. This is an optimal way to quickly and reliably authorize official company correspondence, legal documents, diplomas, ID cards or certificates. The electronic seal is issued for one or two years and is offered together with a cryptographic card (large or SIM), software and optionally a cryptographic card reader.
SIGNIUS S.A.	SIGNIUS Seal – a qualified electronic seal	A solution for qualified automated sealing of documentation in accordance with eIDAS (Eurocert certificate Eurocert or other QTSP certificate), available in various deployment models: as a SaaS service (in the cloud), a dedicated service in a private cloud and in the on-premise model (on-premise deployment).

The list includes only suppliers who are partners of the Trusted Economy Forum CommonSign 2024

✓ Signed
✓ Sealed
✓ Time-stamped
✓ Verified

Authors of the report

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

Legal note:

The opinions contained in the report were issued on the basis of knowledge obtainedfrom market research and the experience of the authors of the report. Authors do not takeresponsibility for decisions taken on the basis of opinions issued as part of the report „REMOTE REMOTE IDENTITY PROOFING, E-SIGNATURE AND E-SEAL IN BUSINESS PRACTICE"