CLOUD SIGNATURE CONSORTIUM

CLOUD SIGNATURE MARKET

EU & GLOBAL PERSPECTIVE

INDUSTRY MARKET REPORT 2025

CSC INDUSTRY MARKET REPORT 2025

THE CLOUD SIGNATURE MARKET: AN EU & GLOBAL PERSPECTIVE

This report has been compiled by Obserwatorium.biz and NIMBUS on behalf of the Cloud Signature Consortium (CSC).
CSC is a global nonprofit association of industry and academic organizations dedicated to developing open standards for cloud-based digital trust services and promoting worldwide interoperability.

We thank all CSC members and other stakeholders in the global digital trust ecosystem for their support and contributions.

Learn more about CSC and our work at cloudsignatureconsortium.org.

Executive Summary

Currently, a variety of technical solutions for electronic signatures are employed worldwide, each grounded in different legal frameworks. On one hand, there are e-signatures based on private keys, recognized only within specific digital services offered by major technology companies. On the other, systems that leverage public key infrastructures which foster interoperability and mutual recognition across commercial and public sectors, forming a robust ecosystem. This ecosystem integrates signature providers, entities that incorporate these solutions into their digital operations, and end-users, often under stringent regulatory oversight. Examples include the UNCITRAL Model Law on Electronic Signatures which has been adopted in more than 40 jurisdictions, the World Trade Organization's (WT) Trade Facilitation Agreement (TFA) accepted by most of WTO members, and the eIDAS regulation of the European Union, which came into force for trust services in 2016. In the following years, UNCITRAL further developed the Signature Law on the basis of eIDAS into a 'Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services', which was published in 2023.

Technically, the spectrum ranges from traditional certificates on physical devices like smartcards to cloud-based signatures, which often allow remote onboarding processes. In many countries, the government provides electronic signatures, typically as part of a broader electronic identification service, using a single electronic identity document as the carrier. Conversely, in other regions, primarily private companies, particularly in the financial sector, deliver these services.

Trust services, and in particular electronic signatures, are poised to become ubiquitous for both businesses and individual consumers globally. For businesses, they offer enhanced recognition in international commerce, while for individuals, their appeal is bolstered by the growing use of remote identification tools and the integration of signatures into digital identity wallets. The primary incentives for adopting e-signatures includes the assurance of cybersecurity in transactions, non-repudiation, and robust legal validation, making them a pivotal element of modern digital interactions. Embracing e-signatures means stepping into a future of secure, efficient, and trusted digital transactions.
Currently, many countries are rolling out electronic ID (eID) projects. To guarantee their widespread acceptance among citizens and businesses, it is essential to integrate electronic signature solutions promptly. Cloud-based e-signatures, which can be adapted to various devices catering to the modern consumer's preference for mobile solutions, could be the most effective method to boost transactions in both public and private e-services. This approach could enable emerging countries to leapfrog traditional market development stages, moving from a lack of digital solutions directly to mobile, electronic signatures. This mirrors the transformation seen two decades ago in Central and Eastern Europe, where nations skipped the use of cheques and directly embraced cutting-edge banking and electronic payment solutions.

To maximize these trends amidst evolving regulations, technological standards, and customer expectations, organizations must focus on collaborating with partners who can adapt and ensure the development of e-signature services according to regulations. The Cloud Signature Consortium exemplifies modularity, flexibility, and the capacity to adapt to legal changes swiftly. A local signature provider, an identity wallet solution, or a commercial entity looking to issue, accept, and recognize various types of electronic signatures - all organizations of these types can gain benefits from a partnership with the Consortium. As one of the participants in the research conducted for this report said – people love standards. But it is important to make sure that the standard adapt to changes at the same pace as businesses and the environment in where it operates.

TABLE OF

CONTENT

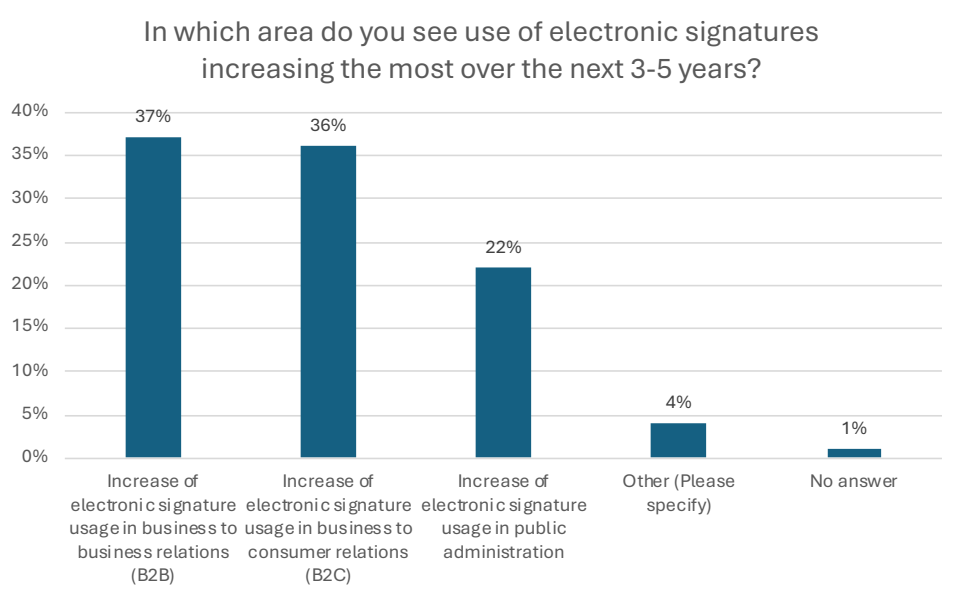
1 CLOUD SIGNATURE MARKET TRENDS IN EUROPEAN AND GLOBAL PERSPECTIVE

1.1. Key market trends in the cloud signature sector

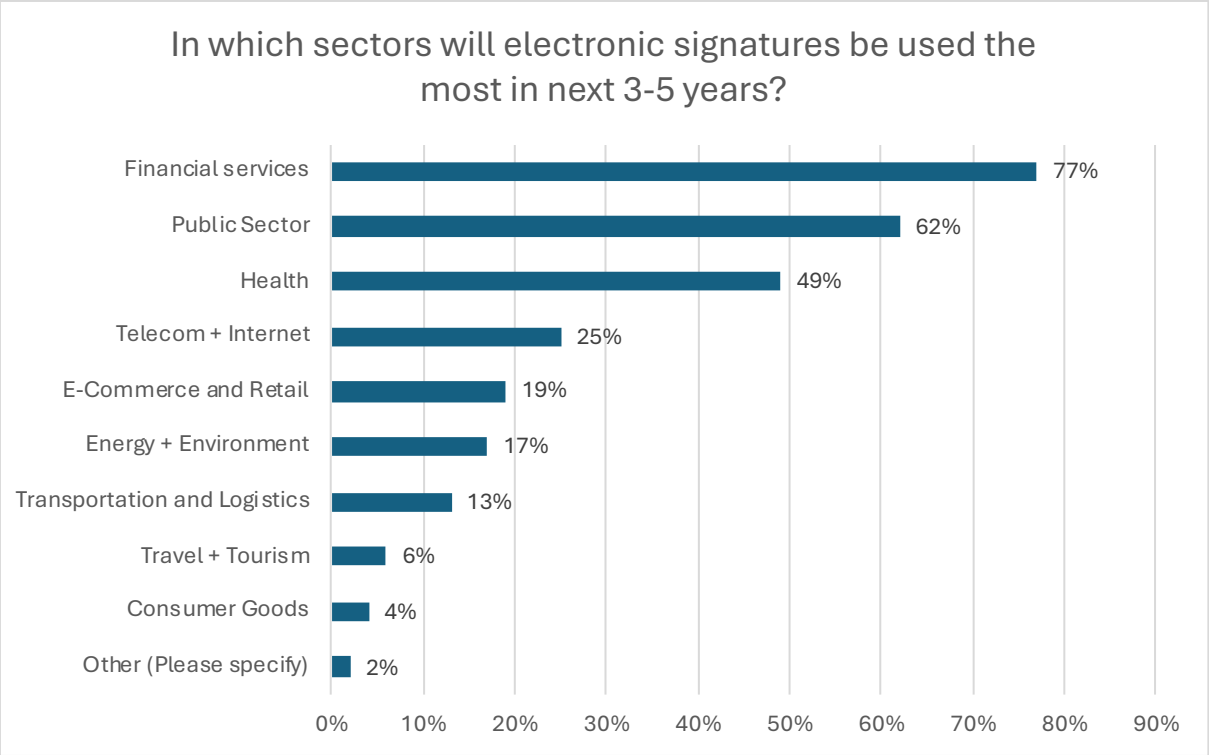
Electronic signatures are one of the most important examples of trust services that ensure the integrity, authenticity, and security of electronic transactions and digital communications. Under the eIDAS regulation, electronic signatures are recognized as qualified and ”normalized” and they are provided by Trust Service Providers (TSP). By successfully undergoing an audit conducted by a conformity assessment body, trust service providers can become certified and receive the status “qualified” by their respective supervisory bodies. This fosters solutions compliant with European law and interoperability.

The global and European market for trust services, particularly electronic signatures, is developing dynamically, primarily due to the active use of trust services in digital transformation processes within enterprises and public administration. The potential for using these solutions remains significant and the market will continue to grow. A survey conducted for this report found that the increase in use cases will be signing via digital wallets (58%) and remote services for electronic signing (42%). Being the most popular trust service based on electronic identification, the electronic signature is not only an autonomous “product” but primarily a key tool in securing and providing proof for processes and electronic transactions, mainly in business-to-business areas, as the majority of respondents indicated in the conducted survey.

Business-to-business relations are the primary areas in which electronic signatures will increase the most over the next 3-5 years according to 37% of the respondents, but they will also play an important role in business-to-customer relations. Electronic signatures are rapidly transforming how transactions are authenticated digitally, offering a key solution for businesses and governments striving to digitize their operations while ensuring security and trust.



Financial services, health, and the public sector are the areas of social and economic activity, in which electronic signatures will be used the most in the next 3-5 years. Available market data indicates an increase in specific sectors, demonstrating improvements in the efficiency of business processes carried out using e-signatures. Estimates for the global e-signature market indicate a 70% - 80% improvement in the efficiency of supported processes. For financial institutions, estimates show a 92% reduction in scanning errors.[1]



3 VARIOUS E-SIGNATURES LEGAL MODELS:

- based on private keys in one ecosystem/ organization (i.e. Big Techs);
- compliant with the specific national rule (i.e. South Africa, Saudi Arabia, India);
- utilizing public keys with mutual interoperability and one legal environment (eIDAS in EU);

Currently various technical solutions for electronic signatures are used worldwide, each based on different legal systems. On the one hand, there are e-signatures based on certificates, which are recognized only within a certain environment of a given digital service provider. Examples for such cases are solutions provided by so-called Big Tech companies or national-specific solutions, like in Japan. On the other hand, systems leveraging public key infrastructure, interoperability, and mutual recognition across commercial and public markets create a connected ecosystem. This ecosystem links signature providers, entities integrating these solutions into their digital processes, and end-users — often operating under strict supervision.

E-SIGNATURE IS CONSIDERED AS A “DIGITAL TRANSFORMATION ENABLER” BY BUSINESS AND PUBLIC ADMINISTRATION

1) https://www.snsinsider.com/reports/e-signature-software-market-1341

A key example of this approach is the eIDAS regulation in the European Union. In many countries citizens and local businesses rely on solutions delivered by the local providers or public administration, ensuring compliance with national-specific rules or laws, for example:

- **South Africa:** the Electronic Communications and Transactions Act 25 of 2002
- **Saudi Arabia:** Royal Decree No. M/8 (Electronic Transactions Law) and the Saudi Arabia Implementing Regulation No. 1/1429
- **India:** Information Technology (Certifying Authorities) Rules, 2000, Digital Signature (End Entity) Rules, 2015; and Information Technology (Use of Electronic Records and Digital Signature) Rules, 2004
- **Vietnam:** Decree 130/2018/ND-CP
- **Philippines:** the Supreme Court of the Philippines' Rules on Electronic Evidence (REE), and the Department of Trade and Industry and the Department of Science and Technology's Joint Administrative Order No. 2 (JAO)

REMOTE ONBOARDING, BASED ON EID SOLUTIONS AND CLOUD E-SIGNATURE AVAILABLE ON MOBILE DEVICES, IS THE BLUEPRINT FOR THE FUTURE, WIDESPREAD SIGNING SOLUTIONS FOR BUSINESS REPRESENTATIVES AND INDIVIDUAL CUSTOMERS.

- **Japan:** the Act on Electronic Signatures and Certification Business (Act No. 102 of May 31, 2000) ("The E-Signature Act")

In many countries, the state is the provider of electronic signatures, often as part of a service linked to electronic identification tools, where for both services the carrier is typically a single electronic identity document. But in these cases, the convenience of onboarding and real penetration within the society is very low (i.e. in Japan, Spain, or Germany). In other markets, primarily private entities are service providers in this area, with the financial sector, such as banks, often playing an important role.

Broad accessibility to obtaining an electronic signature certificate is crucial to the success of both public and private service providers. Remote onboarding, which is one of the main industry trends, increases the accessibility of the service both locally (the ability to sell independently of a dispersed physical distribution network) and internationally (the possibility of building sales processes for customers who are not residents of the country where the provider is based). Increasingly popular eID solutions and schemes support the availability of this way of onboarding. According to the EU market overview, more than half of these services are now offered by qualified trust service providers remotely. In markets such as Italy, Slovakia and Portugal, most services are already available remotely. Spain offers high availability of both traditional and remote registration for an electronic signature certificate. In France, however, the sale of qualified signature certificates onsite still dominates. The most popular identity verification methods for remote onboarding are video-identification (automated or supported by the remote advisor) or use of identification means from governmental or commercial identity providers (i.e. banks).

Another significant business trend is the provision of cloud signatures, by remote management of the signature creation data. Such a solution provides convenient access, usually via commonly available mobile devices, to the signing capability without the need to have an additional carrier or device at the moment. This approach also allows customer-friendly implementation of signing processes in various business procedures, being commonly used in Europe. Based on the available data, it can be stated that already more than 60% of the qualified trust service providers in Europe providing electronic signatures, offer such a service to their customers.

These market trends have created a so-called new-generation of QTSPs, which, regardless of their country of origin and certification, are capable of serving clients throughout the European Union.

THE “NEW GENERATION” OF QUALIFIED E-SIGNATURE PROVIDERS ALLOWS THEIR CUSTOMERS OF ANY COUNTRY TO ONBOARD, SIGN, AND MANAGE THEIR DOCUMENTS FULLY REMOTELY USING USER-FRIENDLY APPLICATIONS AND SEAMLESS PROCESSES.

1.2. Usage of electronic signatures and its perspective in future years

The electronic signature market is currently experiencing significant growth due to several factors. The first is a manifestation of digital transformation initiatives - many countries and organizations are pushing for digitalization to enhance efficiency and service delivery, which increases the demand for electronic signatures. The second key factor is legal recognition, as an increasing number of jurisdictions are granting electronic signatures legal validity. This, in turn, strengthens their adoption in formal and high-stakes transactions. The European Union with its eIDAS regulation is a good example, as it also ensures the interoperability between local providers. Another factor is technology advancements based on standardized APIs which are making electronic signatures more secure and reliable. Electronic signature APIs, such as those from the Cloud Signature Consortium, integrate with various ID verification methods and multiple signing platforms. They enable clients to stay compliant with evolving technical standards, customize business workflows, and ensure system modularity. The last factor is the expansion of ID schemes in many regions - from the European Digital Identity Wallet to US ID and many initiatives driven by local governments in Africa and Asia, such as:

- Ethiopia: Fayda Digital ID
- Kenya: Maisha Namba
- Saudi Arabia: Saudi mResidency
- India: Aadhaar
- Malaysia: MyDigital ID (MYIDSSB)
- Vietnam: The VNeID
- South Korea: Korea Mobile ID
- Philippines: PhilID
- Indonesia: Dukcapil Identitas Kependudukan Digital (IKD)

These initiatives effectively drive electronic signature adoption in these regions by leveraging “bundle strategies,” where e-identity and e-signature are seamlessly provided to citizens and businesses in a single, convenient digital process.

The future of electronic signatures looks promising with ongoing advancements in technology and more strengthened legal frameworks. As electronic signatures integrate with digital identity systems, they are expected to become a standard practice for authenticating a wide range of transactions, further accelerating the digital economy.

Adopting electronic signatures

Regarding the adoption of electronic signatures, the key questions are: What are the most important motivations and barriers to the adoption of electronic signatures within different regions? The primary drivers for adopting electronic signatures include enhanced user experience, security, privacy, and interoperability. These factors cater to the increasing demand for mobile access to digital services. But awareness remains a significant barrier. Many decision-makers are unaware of cloud signature solutions or default to simpler, well-known tools like Adobe Sign, DocuSign and the like, impacting the broader adoption of more secure electronic signatures.

Implementing cloud signatures in regions with varying digital infrastructures requires adaptable strategies that consider local digital maturity. Public administration, struggles with slow process updates and heavy reliance on external consultants, making adoption of new solutions challenging. Emerging requirements, such as free signatures from digital wallets mandated by European frameworks, influence the market dynamics and service offerings. The adaptation involves balancing new regulatory demands with the need to maintain service continuity for existing customers and services sustainability.

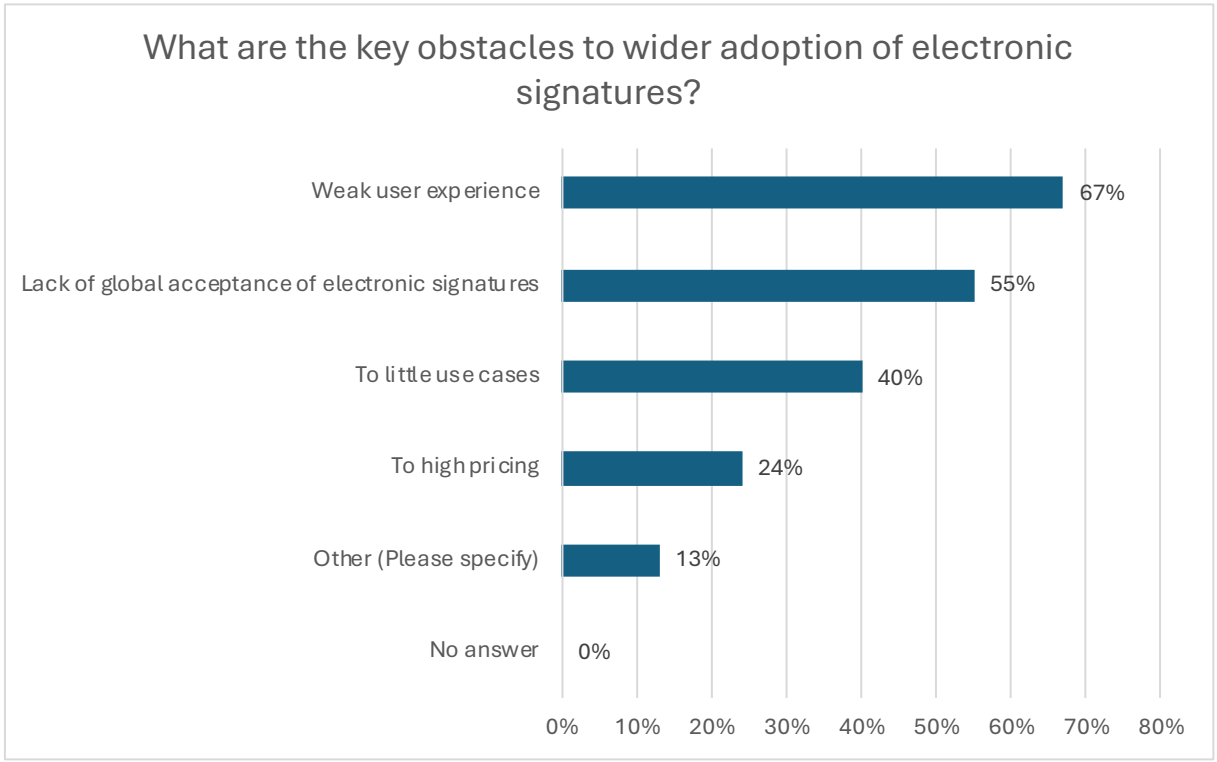
The market for electronic signatures is expected to grow, driven by digital identity initiatives across countries. This growth is anticipated, despite potential regulatory challenges and the need for market education regarding the advantages of advanced signature solutions.

Challenges and considerations

Despite their growing adoption, some challenges need addressing to optimize the benefits of electronic signatures:

- Security Concerns: Ensuring the security and integrity of electronic signatures remains a top priority, as they must prevent forgery and unauthorized access.
- Legal and Regulatory Frameworks: Developing uniform legal standards that recognize and regulate electronic signatures across borders can be complex but is essential for broader acceptance.
- Technological Disparity: There is a need to bridge the gap in technology adoption between developed and developing regions to prevent digital divides.

According to the conducted research, there is another obstacle to electronic signature usage declared by the respondents. It is the user experience of onboarding and signing which is still far below the standard provided by the “digital champions” like Big Tech or most modern digital banks across the world. 67% percent of the respondents indicated that area as the most important barrier. Modern banking relies on electronic services, where remote account opening is the industry standard, credit processes are largely automated, and banks continuously measure customer satisfaction to enhance their offerings. To achieve this, they prioritize both security and user experience, ensuring that most transactions can be performed seamlessly across web platforms, mobile apps, and phone services.



1.3. Various implementations of electronic signature - European, African, Asian, and South American perspectives

Electronic signatures are utilized across a broad spectrum of industries for various purposes:

- **Financial Services:** Facilitating banking transactions and contracts without physical presence. In Romania, qualified electronic signatures are issued by banks within transactional banking, allowing customers to sign contracts for new products such as loans or deposits. In Poland, qualified electronic signatures are used for signing leasing agreements by individuals and the self-employed.
- **Healthcare:** The process of securely handling patient consent and medical records, patient intake forms, patient information and policies can be easily digitized with e-signature usage. With the rise of telemedicine in Africa, South America and Asia, especially in remote areas, electronic signatures are crucial for verifying medical advice and treatment plans provided online. It allows electronic signatures to be used on electronic medical records, electronic prescriptions and other documents allowing doctors to sign and view electronic medical records at any time. This helps in bridging the healthcare access gap in underserved regions.
- **Insurance Processing:** Electronic signatures facilitate the processing of health insurance claims, allowing for quicker verification and approval of claims and reducing paperwork. Electronic signing is often used for signing contracts with customers as well as in the insurance claim settlements.
- **Government:** Enhancing the efficiency of government services to citizens and procurement processes. In many countries, like Indonesia, Saudi Arabia or South Africa, a dedicated e-signature service is used for signing applications and other documents in interactions with public administration. In Europe eIDAS introduced the obligation of the acceptance of qualified electronic signatures provided by European qualified providers in digital processes of public administration. SHECA[2], the first and most experienced certification authority in operation in China, provided electronic signature solutions in such governmental areas as: state tax administration (electronic 'returns, corrections, exemptions and adjustments' services) or logistics (electronic consignment notes - shippers can view the location of carriers in real time and carriers can view the contents of the waybill in real-time).
- **General document processing** – electronic signatures are widely used in electronic document processing platforms. For example, VIDA (Verified Identity for All), a Certification Authority (CA) based in Indonesia, issues legally binding digital identifiers and digital signatures to individuals and institutions. Integration of VIDA E-Stamp services has enhanced Tata.id – a leading provider of document management solutions in Indonesia. VIDA's digital signature services streamlined Tata.id's workflows, while e-stamp ensured legal validation, reducing project timelines through automation and providing clients with legal certainty.

2) https://www.sheca.com/
3) https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Partners/Notarius/DigSigPricing.pdf

- **Education** – electronic signatures are increasingly used in the education sector due to the widespread adoption of digital tools by students and teachers. Notarius[3]- the only Canadian firm that issues trusted signatures recognized by Adobe and Microsoft and certified according to eIDAS standards allows universities to service contracts and leases signed by students, confidentiality agreements, research contracts, intellectual property documents and anything related to business partnerships.
- **Real Estate:** The e-signing process for both preliminary and final contracts in rental agreements and property purchases, as well as for submitting documentation on construction sites, is widely used in many countries. for example in Poland where a new law introduced an electronic construction logbook signed by a qualified electronic signature.

Survey respondents identified user perspective and process ergonomics as critical factors for the successful implementation of electronic signatures. For this report, mystery shopping studies were conducted to evaluate the user onboarding, digital certificate activation, and signing processes of selected cloud-based electronic signature certificates offered by various suppliers. Based on this research some good practices can be provided for such implementations:

- Identity verification using automated video verification and liveness confirmation must be carefully designed for simplicity. If banking credentials are used for identification, the entire process should remain within the same web environment, avoiding unnecessary repetition for customers;
- The use of different tools throughout the process (mobile application, web application) as well as redirection to external services (signature payment, bank account identification) should be reduced as much as possible because it resulted in different language versions as well as a lack of control over the entire process for the user;
- Provided services and user journey should be well described and available in an understandable language for the end user,
- Having 24/7 online customer service for an online purchase is a must, an AI chatbot on the site with predefined ready-made sets of questions to which answers could be quickly generated on key issues at each stage of the user journey proved to be very helpful
- The user should have full control of the signing process, i.e. one could interrupt the process, change the document, select the page to be signed, the specific place on the page, and even the language version of the signature data.

1.4. Market players landscape including CSC members

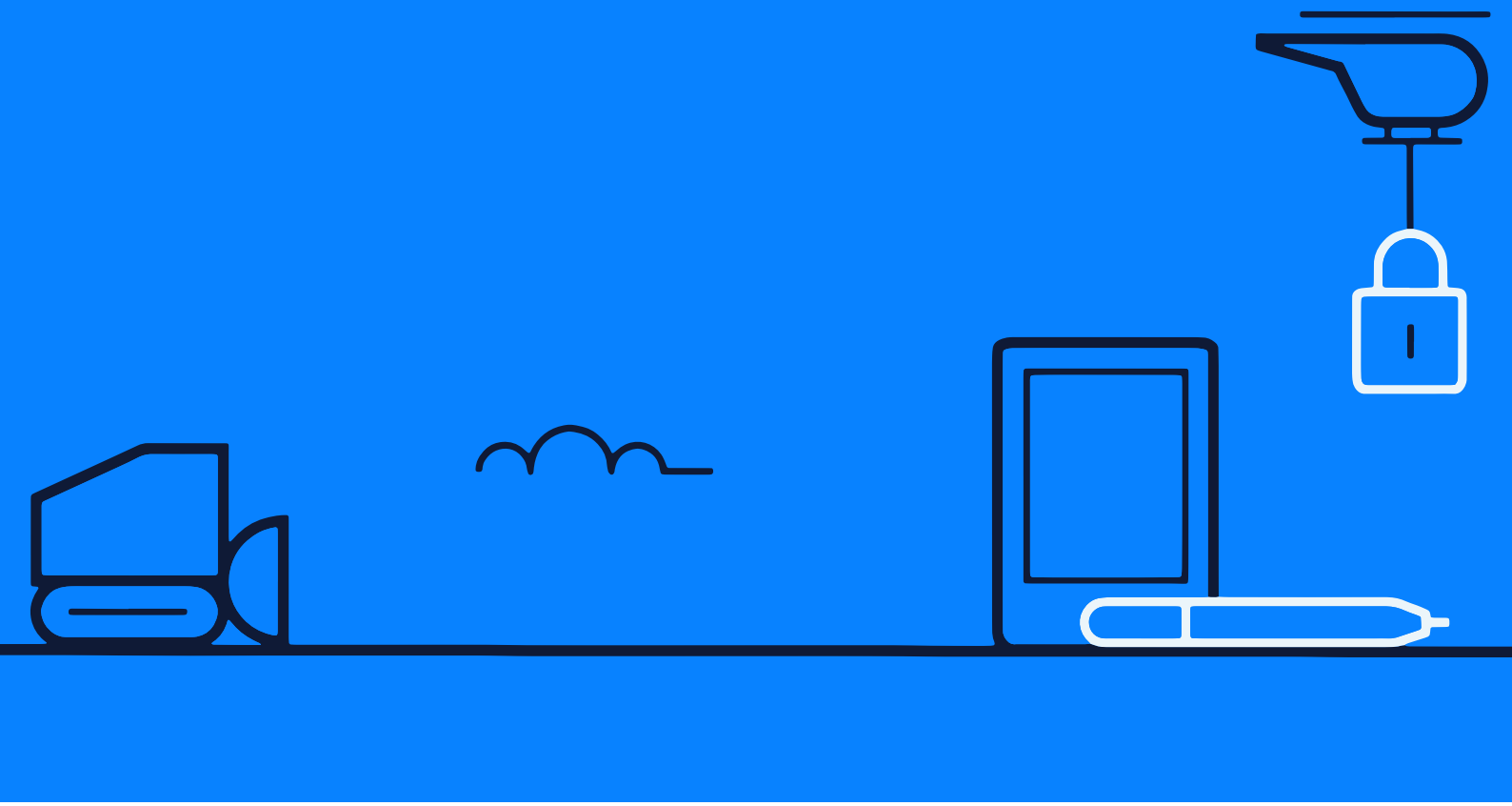
Electronic document signing is increasingly integrated into signature platforms, document management systems (often cloud-based), and custom corporate solutions supporting business processes where making an e-signature is part of the digital process. Electronic identity also plays a significant role in offering digital services – means of electronic identification or video-onboarding processes are both tools for obtaining a qualified certificate or its renewal in a remote formula, and can also be one of the security measures of the business process. As a result of competition, trust service providers serving the traditional market based on hardware solutions, available for purchase or renewal only on-site, are gradually losing market share to entities providing registration (onboarding) and further services remotely. An important element of competitive advantage is the absence of the need to install hardware devices and dedicated software, as well as updating those software. Market share is gained by providers enabling remote processes and allowing clients to manage the documents they sign.

Traditional users of qualified e-signatures, such as regulated entities or officials, often do not choose their certificate provider themselves and typically have low expectations regarding the ease of purchasing and using the product. A significant extension of the natural user base in this area requires, on one hand, solutions with ergonomics similar to those known from the Internet and mobile banking, and on the other hand, significantly expanding the catalogue of use cases, including the ability to use other types of electronic signatures than the qualified signature. The absence of seamless integration for remote signatures within public administration solutions significantly hampers the adoption and use of these services. This lack of functionality creates obstacles for users who may find inconvenience in navigating traditional signing methods, ultimately discouraging them from fully engaging with public administration.

The market for qualified trust service providers (QTSP) in the European Union and other countries in the European Economic Area (Norway, Iceland, and Liechtenstein) shows significant diversity in terms of the number of providers in individual countries - from countries where single companies with this status operate (Finland or Latvia) to countries where there are more than 20 such providers (Italy, France, and Spain). Interoperability is a crucial aspect of these services. Achieving qualified provider status not only enables the provision of trust services but also ensures their legal acceptance across all countries within the community with the same legal effect. This means businesses and individuals can rely on a unified framework for secure digital transactions, fostering cross-border trust and efficiency. The number of providers with QTSP status is steadily increasing - in July 2016, at the time of the introduction of the eIDAS regulation, which sets the rules for the functioning of trust services in the EU, there were 133. The increase of providers to 270 (in European Economic Area - EEA) by the end of January 2025 represents an increase of over 100% in nearly 8.5 years, averaging an annual growth exceeding 10% during this period. Additionally, as part of the process of aligning with European legislation, Ukraine began recognizing trusted services provided by qualified entities from the EU in 2023.

A comprehensive cross-analysis was conducted, gathering detailed data regarding 194 providers (QTSP) in the EEA that offer qualified electronic signature certificates. The majority of them provide both remote registration for their services and cloud-based signature solutions. Some of them can be classified as “traditional” because they implemented the signature based on a smartcard or token possessed by the signatory, and onboarding requires applicant’s physical presence. However, a small group of providers who offered only a signature using a cryptographic smartcard with remote registration was identified. Additionally, there was a slightly larger number of companies that implemented traditional onboarding methods but gave their customers the possibility to use an e-signature in a cloud-based format.

THERE ARE 270 TRUST SERVICE PROVIDERS IN EEA WITH MORE THAN 150 E-SIGNATURE PROVIDERS; MORE THAN 50% OF THEM OFFER CLOUD SIGNATURE SOLUTION.



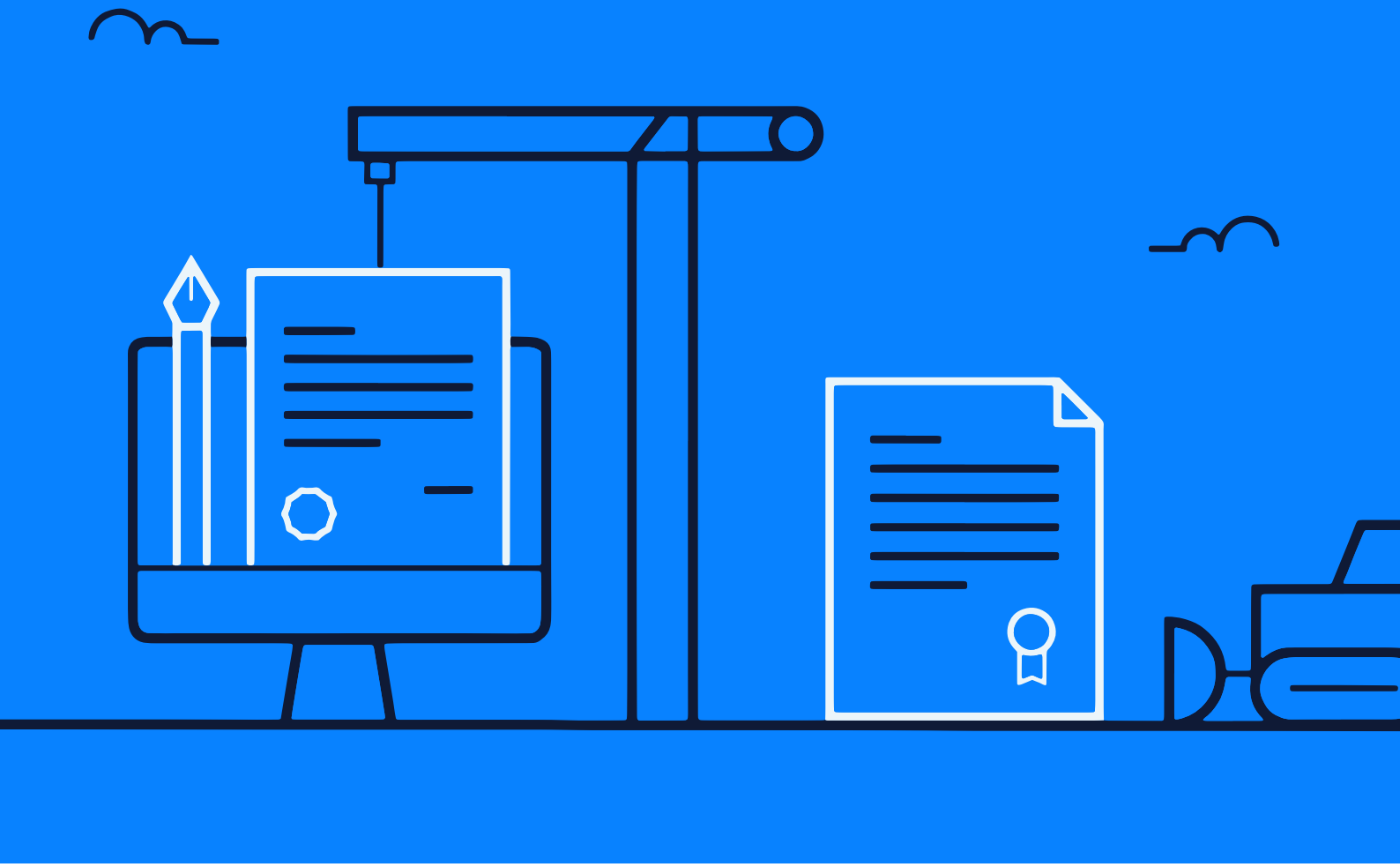
The cloud provides an effective solution to various challenges, particularly in facilitating the immediate migration to cloud-based solutions for mobile devices in situations where such mechanisms were previously unavailable. The European model offers one-shot certificates, e-signatures based on mobile wallets, “freemium” business models, and standardization. Additionally, it supports the use processes of commercial solutions in public sector services.

One characteristic of the analysed market is the significant number of QTSPs (Qualified Trust Service Providers) that have public ownership structures. It has been observed that the highest percentage of public entities is found in France where they make up half of the QTSPs. Spain and Italy also have a considerable proportion, with 25% each. It is worth highlighting the involvement of certain ministries in various countries: France (Economy, Interior, Justice), Italy (Defense), public post offices (France, Germany, Italy), entities associated with notaries (France, Germany, Italy), and regional government entities (Valencia and Catalonia in Spain) as well as the national institutions that are the issuers of securities and banknotes like the Spanish Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) or Polish Security Printing Works (, PWPW).

Brazilian Soluti[4] (CSC Member) is the largest service network in the digital certification market in Brazil, with a presence in more than 3,000 cities. Since 2023, it has offered the IntelliSign digital signature platform acquired from Identity del Peru SA, present in several Latin American countries. Their flagship product is the Bird certificate, a cloud-based signature offered from 2019. The Bird ID issuing process is 100% online and the certificate is renewable for up to 10 years. The Bird ID is integrated with a free solution that enables medical prescribing from any device. In addition to medical procedures, the cloud certificate can be used to access computerized government systems such as e-CAC and Gov.br, as well as to sign contracts, powers of attorney and declarations.

Impression[5] (CSC Member) is a South African solutions provider that since 2011 has helped public sector, financial services, healthcare and retail organizations digitize and democratize their processes so that people can transact

4) https://www.soluti.com.br/
5) https://www.impression-signatures.com/



with them on any device. It offers microservices that can be used by multiple tenants and scaled independently in the geographical area of choice.

Asseco Data Systems[6] (CSC Member) is a Polish QTSP, acting as a subsidiary of Polish-based Asseco Group, one of the biggest IT company in Central and Eastern Europe. This vendor provides customers with an electronic signature as part of a complete suite of trust services, including validation and e-delivery services. This package, combined with a cloud-based signing platform, enables business clients to conveniently manage the entire lifecycle of an electronic document.

emdha[7] Trust Service Provider (TSP) (CSC Member) is operating under the Saudi National Root CA, offering trust services ranging from Online Digital Signatures, Digital Certificates, and Timestamp Services. Entities covering most of the use-cases and needs of KSA digital transformation aligning with the Saudi Digital Vision 2030, offering two different models one offered to the Semi-Govt/Government Agencies and Private Organizations that rely on National KYC sources/Trusted KYC source and to banks regulated by SAMA (Central Bank) and the second one which is offered to all Organizations and Individuals, as a mechanism to digitally sign documents with a legally binding status in the KSA as per the Saudi eTransaction law.

6) https://www.assecods.pl/
7) https://www.emdha.sa/

2 CLOUD SIGNATURE MARKET TRENDS IN EUROPEAN AND GLOBAL PERSPECTIVE

2.1. Cases of remote signature usage in business and public administration - ”How can we reduce the secure and trusted digitalization gap?”

Every year, the market for remote digital signatures experiences significant growth, reflecting the increasing demand for streamlined and secure ways to execute documents and contracts electronically. As technology advances, the list of processes and areas where one can use e-signatures is constantly growing. The remote signatures are now commonly deployed not only in the private sector for transactions and contracts but also within public administration to enhance efficiency and accessibility in governmental procedures. This growing integration of remote signatures is transforming how organizations operate, making signature processes faster and more efficient than ever before.

> In an increasingly digital world, the ability to sign documents remotely has become a fundamental requirement for both businesses and public administration.

This chapter presents real-world use cases showcasing their role in streamlining workflows, reducing costs, and ensuring regulatory compliance. Readers will gain insights into the diverse applications of remote signatures, including contract management, financial transactions, citizen services, and regulatory compliance. Each case study highlights the challenges faced, the solutions implemented, and achieved benefits, providing a comprehensive overview of the growing role of remote signatures in modern business and governance.

Signicat & Entercard[8]

Signicat helped one of the big, international payment card providers -Entercard - increase their conversion rate by automating cross-border onboarding.

Entercard sought effortless and easily verifiable digital identity authentication and e-signing solutions accessible through a unified API across Norway, Sweden, Finland and Denmark.

The cooperation with Signicat brought satisfactory results. Entercard modernized processes, improved security and optimization of business operations, while ensuring compliance with regulations in force in various countries. Conversion rates increased from 63% to 82%. The fully automated onboarding time per customer reduced from days to minutes. All signing was done using electronic signatures from Signicat. The result is a fully compliant solution, adapted to local and international regulations.

D-TRUST in Healthcare Sector[9]

As the healthcare sector becomes increasingly digital, healthcare facilities are striving to streamline their processes by eliminating paper documentation and

8) https://www.signicat.com/customers/entercard
9) https://www.d-trust.net/en/solutions/ti-remote-signature

introducing electronic solutions. One key element of this process is the ability for healthcare staff to securely and legally bind electronic documents. In Germany, healthcare staff had to use a physical Healthcare Professional Card (eHBA) and a card reader with a PIN to sign electronic documents. This approach was associated with several challenges: hardware limitations, complexity of processes, high cost.

D-Trust's TI Remote Signature allowed medical staff to sign documents remotely, without the need for physical cards or additional hardware. It is an eIDAS-compliant solution with two-factor authentication and is usable on various devices using an Attribute in the certificates confirming the licence to practise medicine. TI Remote Signature optimizes document workflows in healthcare, ensuring secure and compliant digital signing while improving operational efficiency.

Qualified Electronic Signatures in public administration in Poland

Public administration sought to streamline processes through digitalization and needed a reliable solution for signing electronic documents. There are many processes in Poland where qualified electronic signatures are mandatory – the catalogue of e-signature applications in offices includes at least several dozen use cases. It can be used to sign documents for the Tax Office, Social Insurance Institution, National Court Register, public procurement offers and many others.

All TSPs provided qualified electronic signatures, enabling officials to securely and efficiently sign administrative decisions, contracts and other documents. As a result, processes became faster, and the costs associated with handling paper documents were reduced. QES contributed to streamlining administrative processes and increasing data security.

Adobe Acrobat Sign (not QES) in US public administration[10].

The Utah state government implemented Adobe Acrobat Sign as a tool for signing and managing electronic documents, which was intended to improve the remote work of officials. Adobe Acrobat Sign provides an electronic signature solution, which enables officials to sign documents remotely without the need for a physical presence. The platform relies on two main types of electronic signatures: basic electronic signatures and digital signatures. The former is the simplest form of e-signature, where the signer's identity is typically confirmed via email, with the possibility of additional authentication methods, such as a one-time password (OTP) sent to a mobile device. The latter, digital signatures, offers a higher level of security by using digital certificates issued by trusted certification authorities, ensuring stronger authentication and document integrity through cryptographic methods. Additionally, the solution brought several other benefits: faster document approval, the possibility of full telework of the administration, saving time and operating costs, reducing paper consumption and CO_2 emissions and greater readiness for crisis situations.

Namirial & Guatemala Chamber of Commerce

The Guatemala Chamber of Commerce chose PKIaaS (Namirial's product) for its full range of services. By using a cloud-based service and a pay-per-use model, they gained access to all key elements of the PKI infrastructure offered by Namirial. This included a dedicated Certificate Authority with digital certificates issued by an organization, a Registration Authority, a Validation Authority, and a Time Stamp Authority, a Centralized Certificate Custody Service (CCCS), an Electronic Signature Service (ESS), and Electronic Signature Validation and Verification (VOL). This solution brought numerous benefits in terms of time and cost-efficiency, security and technological advancement. The government uses PKIaaS to enable in-depth cross-sector e-government initiatives and to provide various social and economic services to businesses and citizens.

The listed use case offer a good overview over different best practices for electronic signatures in various sectors. As well as the mentioned providers, there are many more on the market that offer similar services. A detailed description of each one of them would go beyond the scope of this study.

8) https://blog.adobe.com/en/publish/2020/04/27/the-state-of-utah-uses-adobe-sign-to-accelerate-telework-during-crisis, https://helpx.adobe.com/pl/sign/config/digital-signatures/overview.html?utm_source=chatgpt.com

2.2. How to implement cloud signatures within your company as a digitalization tool

Electronic signatures as a tool are an invaluable business enabler, however proper preparation is a key part of implementation for any organization. Implemented well, electronic signatures can be a shift in how organizations handle documents, processes, and security. Skipping or dismissing this step may result in technical, legal, or operational problems and challenges that could undermine the potential benefits.

Below are brief descriptions of the phases.

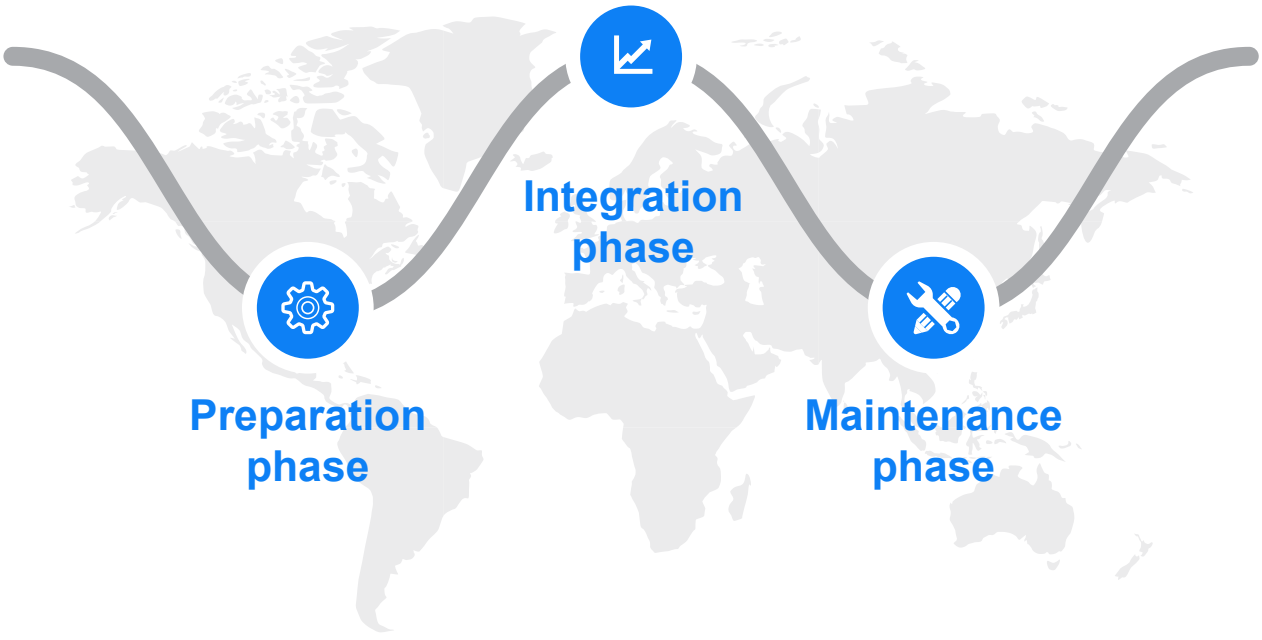
1. Preparation phase

Preparation should begin with a thorough **analysis** of the company's legal requirements, business processes and any potential international environments. Analysing these factors is crucial for proper selection of an electronic signature solution that fits all the requirements. Depending on the region, some specific standards and regulatory frameworks might apply, such as the eIDAS regulation in the European Union or the ESIGN Act in the United States. A lack of compliance with these standards could render electronic signatures invalid, exposing the organization to legal disputes or administrative setbacks.

The second, equally crucial step is a thorough analysis of the institution's business, usability, workflows, security needs, and its broader ecosystem, including customers, partners, and suppliers. The implemented solutions must not only be acceptable to these stakeholders but also offer additional benefits or extra value that alternatives do not provide.

Once all the necessary perspectives are known and understood, a design process can begin. Scheduling, planning and testing ensures a smooth transition across the organization. This includes integrating the solution into existing systems, training employees, and rethinking workflows to accommodate digital processes. A rushed or unplanned implementation can lead to confusion, resistance from staff, and inefficiencies that negate the potential advantages of using electronic signatures.

eSignature implementation process can be summed up in three phases:



It is important for the solution to meet the organization's needs and requirements as much possible, this includes the following aspects:

- **Usability and user experience** – *Is it user friendly? How difficult is it to use? Can first time users use it on their own?*
- **Interoperability and flexibility** – *Does it fit standards and regulatory frameworks? Is it recognized and usable for a variety of use cases? Can it be used/ recognized outside of the country?*
- **Scalability** – *Can it be extended to different processes and workflows?*
- **Functionality** – *Does it fulfil all the institution's needs?*
- **Cost** – *How much does it cost to run it? How is company charged for the signatures? How will costs change if signatures are extended to additional processes or additional users?*
- **Audits** - *Is an external audit needed, e.g. EN 319 401, EN 319 411 requirements under EN 319 403 audit for Qualified Trust Service Provider in European Union.*

2. Integration phase

Once a supplier has been selected, the next phase is the implementation of the solution within the organization. A well-structured approach ensures effective integration with existing workflows, employee readiness, and clear communication with stakeholders. A phased and methodical rollout helps in minimizing disruptions while maximizing efficiency.

Before the actual integration, a pilot implementation is recommended. This serves as an opportunity to test the new workflow in a controlled environment, typically in a single department or process. A pilot program allows the organization to assess the technology's performance in real-world scenarios, gather feedback from users, and identify any challenges or technical issues.

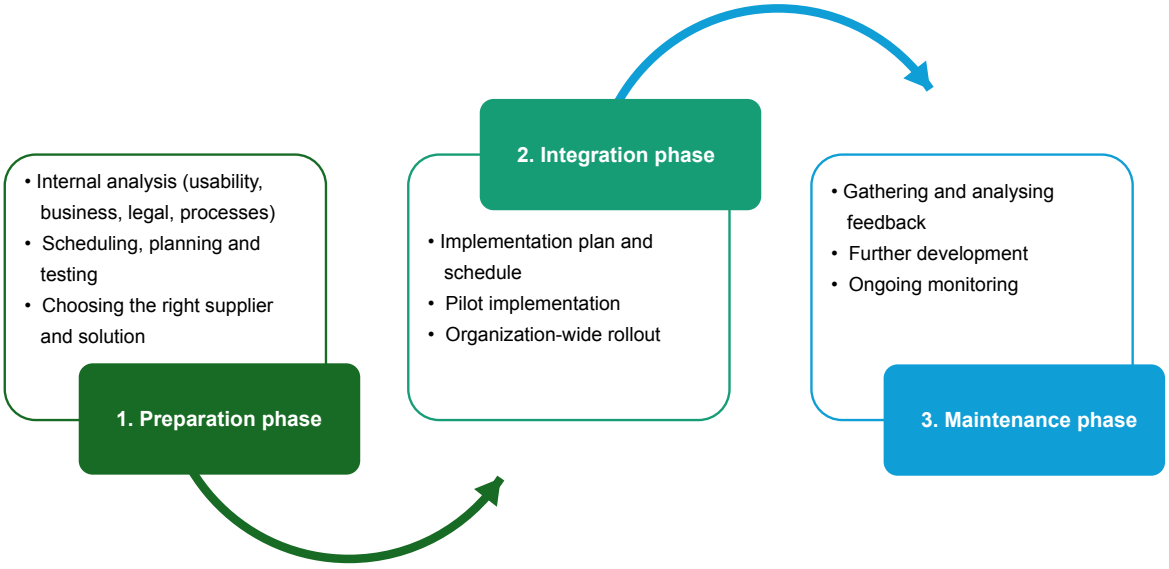
After successfully completing the pilot phase and necessary adjustments have been made, the final version of the electronic signature solution can be rolled out across the organization; this applies to both internal processes and customer-facing processes. In certain regions additional requirements may apply before the rollout can occur, most notably a successful audit of the implemented solution.

Clear communication plays a vital role in the success of the rollout. Employees should be kept informed, while external stakeholders, including clients and business partners, should be notified through official announcements, website updates, and social media. Ongoing training and support should continue even after implementation to ensure employees remain confident in using the system.

3. Maintenance phase

Gathering and analysing feedback is an essential part of keeping processes, products and workflows effective and efficient in the long-term. Input from employees, customers, and partners can highlight challenges, technical issues, or problems. Surveys, helpdesk reports, and system analytics should be reviewed to assess user experience and adoption rates. Outside audits and usability analytics can provide an independent, objective perspective based on metrics, heuristics and best practices.

As the organization grows comfortable with electronic signatures, extending their use to new processes and/or departments may be worth considering.



2.3. Potential of cloud signatures in international trade

Cloud signatures are a key component of the ongoing revolution in how business is conducted at both national and international levels. Today electronic signatures are more accessible than ever before and they can significantly impact many aspects of trade. Leveraging them can streamline processes, increase efficiency, security, and cost savings in cross-border transactions.

Facilitation of faster contract execution. Traditional trade agreements often involve multiple stakeholders across different countries, requiring extensive paperwork and causing delays due to physical document transfers. Cloud-based electronic signatures enable parties to sign contracts remotely in real time, reducing transaction times from weeks to minutes. This acceleration enhances supply chain operations, minimizes risks related to shipment delays, and improves overall business agility.

Security. Strong encryption and authentication mechanisms can ensure integrity and authenticity of signed documents beyond any doubt, unlike physical signatures.

Cost efficiency. International trade often involves significant expenses related to document handling, courier services, and administrative efforts. By eliminating paper-based workflows, businesses reduce overhead costs while also contributing to sustainability efforts. Additionally electronic documentation reduces waste and the carbon footprint associated with traditional logistics, aligning with global environmental goals.

Adoption of cloud signatures is in part driven by global trade policies and legal frameworks that encourage digital transformation and ensure legal compliance:

- **The European Digital Identity Framework** foresees the integration of electronic signatures and seals into the European Digital Identity Wallet. In the Commission Implementing Regulation laying down rules for the integrity and core functionalities of European Digital Identity Wallets stipulates that signature and seal formats supported by signature creation applications, as referred to in Article 12, shall use an application programming interface that supports the Cloud Signature Consortium (CSC) specification (API v2.0). This explicit reference to the CSC API v2.0 underscores the EU's commitment to promoting interoperability, cross-border recognition of digital signatures, and the broader adoption of secure, cloud-based solutions—key enablers of digital transformation across public and private sectors.
- **UNCITRAL Model Law on Electronic Signatures (MLES in 2001)** offers a framework for national legislation and legal recognition of electronic signatures. It allows assurance that electronic signatures are enforceable and accepted in courts, eliminating uncertainties associated with digital transactions. MLES-based laws have been adopted or have influenced legislation in 40 countries across 42 jurisdictions[11]. The European Union (EU) has not directly adopted the UNCITRAL Model Law on Electronic Signatures (MLES) from 2001. Instead, the EU has established its own comprehensive framework for electronic signatures through the eIDAS since 2012. From 2017 to 2023 the United Nations Commission on International Trade Law Working Group IV: Electronic Commerce developed the "Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services" initiated by many EU Member states. The new Model Law is very similar to eIDAS 2014, but uses the term "reliable" instead of "qualified" Trust Services. While the UNCITRAL Model Law serves as a reference, eIDAS is enforceable within the EU,

11) United Nations, Status: UNCITRAL Model Law on Electronic Signatures, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status

ensuring that electronic signatures are recognized uniformly across the entire EU and EEA.

- **World Trade Organization's (WT) Trade Facilitation Agreement (TFA)** promotes the use of paperless trade processes to enhance efficiency in customs clearance and cross-border trade. Additionally, many governments and financial institutions recognize the validity of electronic signatures, fostering their use in contracts, invoices, and shipping documents. 157 out of the 164 WTO members have ratified the Trade TFA[12]

- **The Global Legal Entity Identifier Foundation (GLEIF)** takes a different technical approach, focusing not primarily on signatures but on clarifying the role of representation authority in the authentication process of organizations. With ISO 5009, GLEIF established a standardized framework to verify the representation power of individuals acting on behalf of an organization via an Official Organizational Roles (OOR) Code List. This ensures that digital identity systems, including electronic and cloud-based signatures, can reliably confirm not only the existence of an entity (via the LEI via X.509 certificates, ISO 17442-2:2020) but also specify the official roles of persons representing their organizations. The latter GLEIF plans to leverage in the verifiable LEI (vLEI) role credentials (ISO 17442-3:2024).

Despite the progress, there are still challenges in achieving universal acceptance of cloud signatures. Some countries still lack clear regulatory frameworks for digital signatures, leading to legal uncertainties for cross-border transactions. Additionally, there is no uniform and globally accepted legal and technological standard. These issues can be addressed by utilizing standardized APIs and by following the example of more advanced regions such as the EU, which led the way for the implementation of consistent, region-wide legislation. The Cloud Signature Consortium´s API is thus an important standard that enhances global interoperability and the security of electronic signatures.

12) The World Trade Organization, Ratifications List, https://tfadatabase.org/en/ratifications

3 IMPACT OF THE AMENDED EIDAS

Introduction

The amendment to the eIDAS Regulation (commonly referred to as eIDAS 2.0) introduces a new model of electronic identification and trust services, which significantly impacts the functioning of both the public and private sectors in the European Union. The eIDAS amendment establishes the European Digital Identity Framework.

3.1. The Amended eIDAS Regulation and its Legal Impact on eID and Trust Services in Europe

In 2021 the European Commission announced the revision of the eIDAS regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC). The revision aims to establish a European Digital Identity framework, providing a harmonized legal basis for all EU member states to implement their digital eID and additional identity-related attributes through a Digital Identity Wallet. The updated regulation came into force in May 2024, with accompanying implementing acts set to be published by the end of May 2025.

The eIDAS regulation from 2014 introduced qualified trust services to enable harmonized cross-border digital transactions and a notification scheme for the member states to recognize their national eIDs. The latter lead to over 25 notified eID schemes in Europe but not to interoperable and cross-border usable solutions. Thus, the revised EUDI framework aims at defining rules and technical standards in order to enable interoperable and secure ID solutions across Europe. While the eIDAS regulation of 2014 managed to establish a market for qualified trust services, its potential has not fully been untapped. Especially in the public sector and among individuals, qualified electronic seals and signatures remain underutilized. This varies across member states, but overall, the legal separation of identities and trust services has posed challenges to the full realization of the single digital market, as well as to both private and public use cases. Thus, the European Digital Identity wallet aims to combine both, eIDs and trust services.

Every member state must provide their citizens and organizations with a European digital identity wallet at the end of 2026. Each member state is free to decide whether to develop a state-run solution, outsource it to the private sector, or pursue both approaches. Either way, the EUDI wallet needs to be provided free of charge and its usage by the user remains voluntarily.

In line with the principle of national sovereignty, each member state's eID will only be stored in the wallet notified by member state. This means, for example, that without Spain's consent, a Spanish eID cannot be stored in a German wallet. However, a Spanish EUDI Wallet must be recognized in Germany and remain fully functional across both public and private use cases. This will be guaranteed through common standards that are defined by various European and international standardization organizations of which some are partly referenced in the implementing regulations, thus legally binding by law.

The European Digital Identity Wallet is both a product and a service, enabling users to securely store their national eID and identity-related attributes, share them with relying parties as needed, and use them for online and offline authentication, as well as for qualified electronic signatures and seals.

The introduction of free qualified electronic signatures (QES) for non-commercial usage could significantly increase their adoption, leading to a situation where use of qualified electronic signatures become the standard for electronic transactions, much like an ID card is a recognized travel document across Europe. The exact implementation of the free-of-charge QES is yet to be defined by the implementing acts. However, beyond the benefits for individuals and its potentially wider market adoption, there are still open questions regarding its impact on Qualified Trust Service Providers (QTSPs) and market development. In conducted survey , many QTSPs expressed their concerns regarding this intervention in the market.

Providing a free of charge electronic signature for non-professional purposes to every European Digital Identity Wallet holder may help raise user awareness of the tool and the benefits of its use. However, it is crucial to enable the creation of such signatures and ensure their recognition and acceptance, particularly by public entities. The new regulation stipulates that the digital identity wallet will be used in both public and private services, and its acceptance as a means of authentication will become mandatory for financial institutions, media providers and “very large operators” that require a strong customer authentication for their services. This reduces dependencies and allows the user to choose a European, secure and private authentication.

Equally important is the ability to develop models for qualified electronic signature where the commercial market can pay for signatures when needed, fostering the growth and competitiveness of solutions available to citizens using the wallet. A key factor for further development is establishing an ecosystem that supports the growth of paid qualified electronic signatures for commercial purposes. By combining qualified signatures with attributes the wallet provides, a wide range of business needs can be effectively addressed.

3.2. Possible Scenarios of the New Rules in Terms of QTSP Business Attitude and Possible Remote Signatures (RS) Proliferation

The changes introduced by the amended eIDAS Regulation present new challenges for Qualified Trust Service Providers (QTSPs). One key issue is the impact of free qualified signatures on **the business model of trust service providers**.

At least three market development scenarios are possible:

- **"Loose-Loose" Model** – A lack of willingness among commercial Trust Service Providers to offer free signatures, coupled with an absence of state-developed solutions, could render the provision of the regulation ineffective.
- **State-issued Model** – The creation of signature solutions by public administration. If Member States choose to provide free qualified signatures to citizens through state-run qualified service centers, it could limit the role of commercial providers, reducing innovation and competition in the market.
- **Open Market Model** – In this approach, qualified providers enter into public-private partnerships with public administration, where transparently selected providers offer free signatures for private use by individuals. The compensation for the services should come from governments. This approach could balance public interests with the private sector's viability.

While the concept of free qualified signatures for individuals ensures that they can sign documents at no personal cost, it does not eliminate the need for a designated payer to cover the associated service costs. It is essential to consider who should bear this financial responsibility, particularly in commercial and governmental interactions. For example, in cases where individuals sign credit agreements with financial institutions or submit official documents to public offices, the cost of the signature should arguably be covered by the professional entity requesting the signed document. This approach would ensure sustainable funding for trust services while maintaining accessibility for individuals.

Many companies see an opportunity to extend remote signing services beyond the EU, particularly in countries that adopt the European regulatory models. A broader market presence is expected to positively impact service pricing and shift provider strategies toward more flexible, subscription-based business models and integrations with mobile wallets.

The role of public administration in trust service provisioning remains crucial. Historically, government entities have not been the best providers of electronic services due to resource constraints and limited flexibility in adapting to users' evolving needs. Thus, finding a balance between the state's role as an identity provider and the private sector's capacity to deliver innovative, competitive solutions will be essential.

3.3. Remote signatures, European Digital Identity Wallet and new technical standards

The European Digital Identity Wallet requires **a unified technical standard** to ensure interoperability and secure credential storage. Currently, there is no certified model that allows **local storage of cryptographic keys** on users' mobile devices (phones). This is due to:

- The diversity of operating system and hardware providers,
- The necessity to comply with the EU's high security standards.

An alternative is **remote signatures**, which eliminate the need for local cryptographic key storage. Aligning **ETSI standards** with the EUDI Wallet's requirements will be critical to its success. **The Cloud Signature Consortium (CSC)** standard is particularly relevant here, as it could form the basis of interactions between wallet applications and signature service providers. Efforts are currently underway to **validate and integrate the CSC standard** as a solution for supporting remote signatures.

New technical standards, such as Cloud Signature 2.1.0.1 Architectures and protocols for remote signature applications (CSC API), enable greater interoperability and modularity in electronic signature services, allowing providers to integrate with various e-identification systems.

3.4. QCS implementation in the European Digital Identity Framework

There is growing interest in implementing **remote signatures** in the context of mobile wallets, which could influence the provision of trust services in Europe and beyond. As a result, remote signatures are becoming a key element of the European Digital Identity Framework ecosystem.

The EUDI Wallet is a pivotal initiative aimed at providing EU citizens and businesses with a secure and standardized digital identity solution. A key feature of the EUDI Wallet is its capability to facilitate the creation of Qualified Electronic Signatures. The integration of the Cloud Signature Consortium (CSC) API plays a crucial role in enabling this functionality.

The amended eIDAS regulation includes the requirement (under Article 5a(5)(a)(xi)) for the EUDI Wallet to support "common protocols and interfaces" for the creation of QES by means of a QSCD. The Implementing Regulation on the "integrity and core functionalities" of the EUDI Wallet published by the European Commission in 2024 states that the application programming interface of signature creation applications integrated into wallet instances shall support the Cloud Signature Consortium (CSC) specification, version 2.0.

The Cloud Signature Consortium (CSC) API already provides the interface between the e-signing platform and the QSCD for remote signing with QES, and it will continue to do so when the EUDI Wallet is made available to citizens.

The CSC API offers a standardized interface that ensures compatibility between various digital signature services and platforms. By incorporating the CSC API, the EUDI Wallet can seamlessly interact with different Qualified Trust Service Providers and their remote Qualified Signature Creation Devices (QSCDs). This interoperability is essential for a unified digital identity framework across the EU, allowing users to sign documents remotely with QES, regardless of the service provider or platform they choose.

source: CSC[13]

13) https://cloudsignatureconsortium.org/wp-content/uploads/2024/10/CSC-White-Paper-The-role-of-the-Cloud-Signature-Consortium-API-in-the-new-European-digital-identity-framework-and-beyond.pdf

The CSC API's design accommodates future advancements in digital signature technology and evolving regulatory requirements. Its flexibility ensures that the EUDI Wallet remains adaptable to new use cases and technological developments. Moreover, the CSC API's global recognition facilitates potential integration with digital identity frameworks beyond the EU.

The Architecture and Reference Framework[14] for the EUDI Wallet outlines integration models for the Cloud Signature Consortium (CSC) API to facilitate Qualified Electronic Signatures. These models ensure secure and interoperable digital signing services within the EUDI Wallet ecosystem.

In this model, the EUDI Wallet interacts with a remote QSCD managed by a Qualified Trust Service Provider. The CSC API standardizes the communication between the Wallet and the remote QSCD, enabling users to create QES without requiring local signature creation devices and drivers installation. This approach enhances user convenience while maintaining high security standards.

Integrating web-based Signature Creation Applications with digital identity wallets enhances the security and user control in electronic signature processes. In this setup, the web application manages the signing process. The wallet, acting as a personal tool enabling signatory sole control, manages the user's digital identities and credentials, ensuring that the private keys are used only on the explicit EU Wallet holder request. Upon receiving the request, the wallet prompts the user for authorization, and once granted, it utilizes the user's private key stored on remote QSCD to generate the electronic signature. The signed document is then returned to the web application for further processing or distribution. By implementing a unified standard for digital wallets, users will be able to use qualified signatures intuitively and securely, accelerating the digitization of public and commercial services.

Key benefits of using the CSC API within the EU Digital Identity Framework:

- it enables seamless **integration with digital identity providers and EUDI wallets**,
- it allows businesses to maintain existing without requiring significant changes,
- **it assists commercial QTSPs in adapting quickly to new developments and circumstances.**

Organizations such as the Cloud Signature Consortium could play a crucial role in harmonizing the market and ensuring interoperability between trust service providers and digital wallets.

The Cloud Signature Consortium (CSC) standard allows for secure document signing without the need for a physical key storage device. Integrating this solution with the EUDI Wallet will:

- **Enable widespread adoption of qualified signatures** without complex installations,
- **Ensure consistency with existing eIDAS regulations,**
- **Facilitate easy integration with public and private sector systems.**

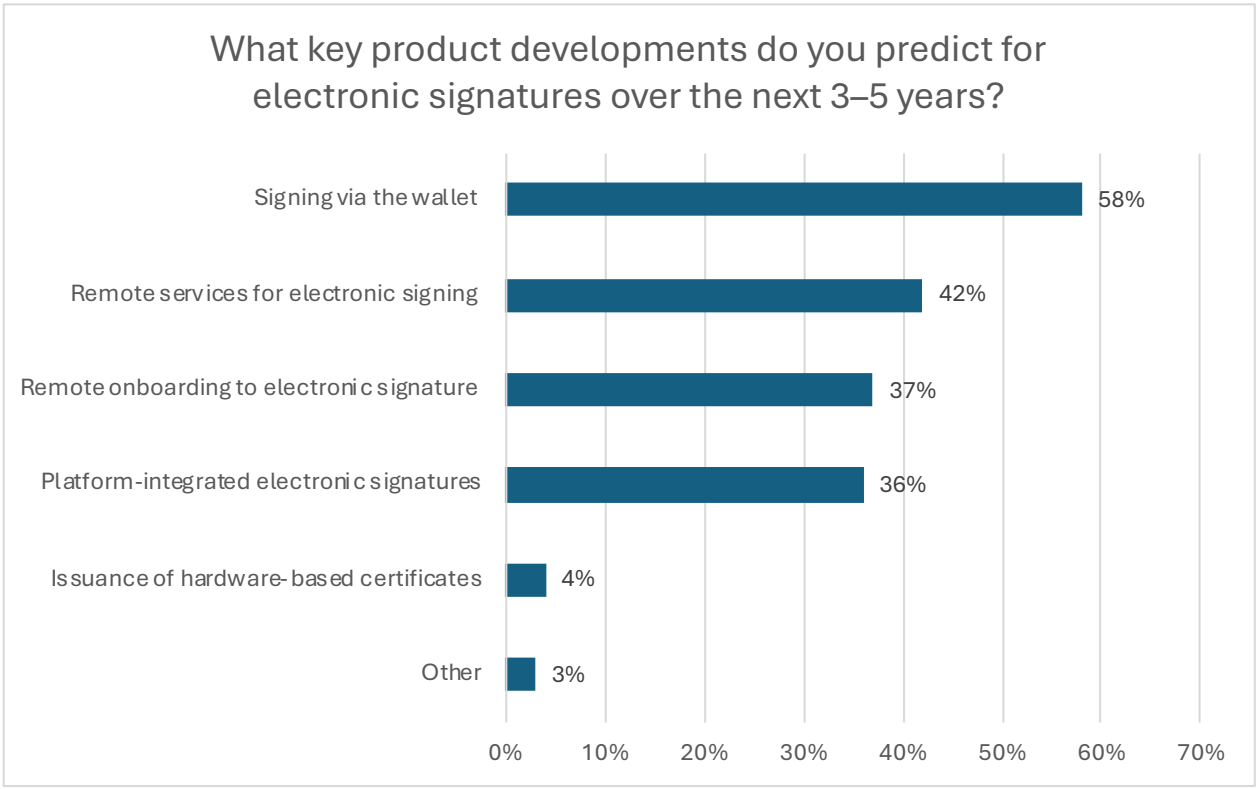
14) https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/

4 EUROPEAN AND GLOBAL MARKET TRENDS 2025 +

4.1. Projection of the e-signatures market development based on the market research conducted for the report – main trends of the market in 2025 +

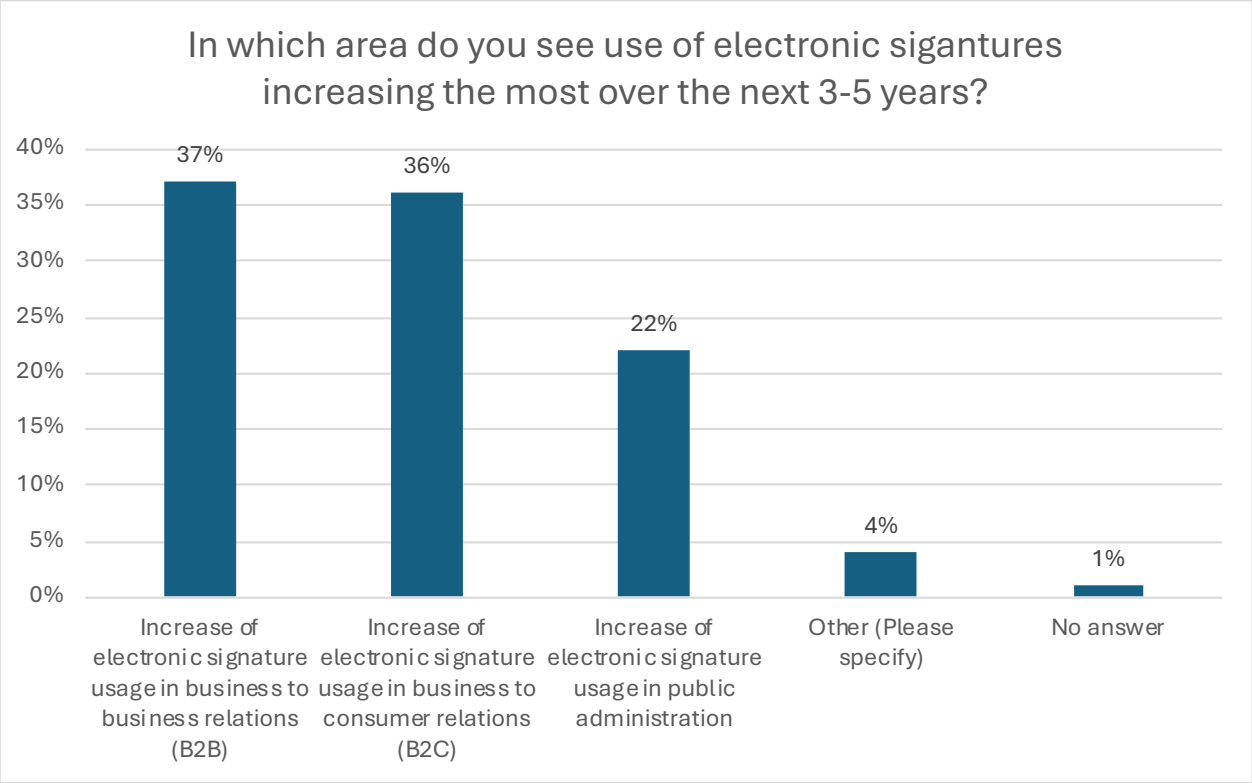
The Analysis of the data conducted for the report regarding the electronic signature market highlights several key trends that may define its development in the forthcoming years. In the online survey Present and Future of the European and Global Remote Signature Market, 100 respondents participated. The analysis of the regions in which their companies operate or cooperate showed that Europe is the dominant area of activity – 78% of responses referred to EU countries, while 23% concerned non-EU countries. Japan (19%) and South America (18%) also received significant mentions. The lowest number of responses related to China (7%) and Central Asia (4%)[15].

Over the next 3–5 years, the most anticipated innovation will be the integration of the signing process with digital wallets, as indicated by 58% of respondents. The second most popular solution is remote signing services, which received 42% of responses. Another significant trend is the remote issuance of electronic signature certificates (37%) and platform-integrated signatures (36%).

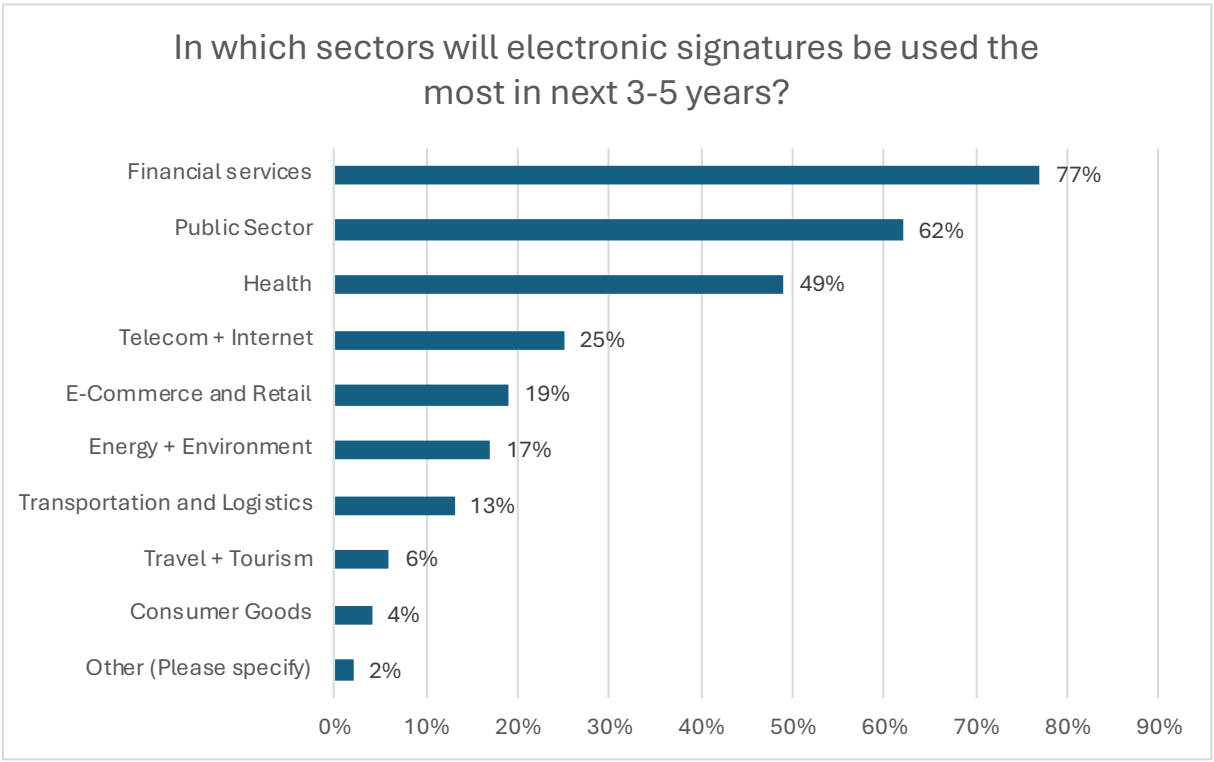


15) The Question 3 focuses on the region in which the respondent's company primarily operates/ cooperates In the multiple-choice question, a total of 216 responses were provided by 100 respondents.

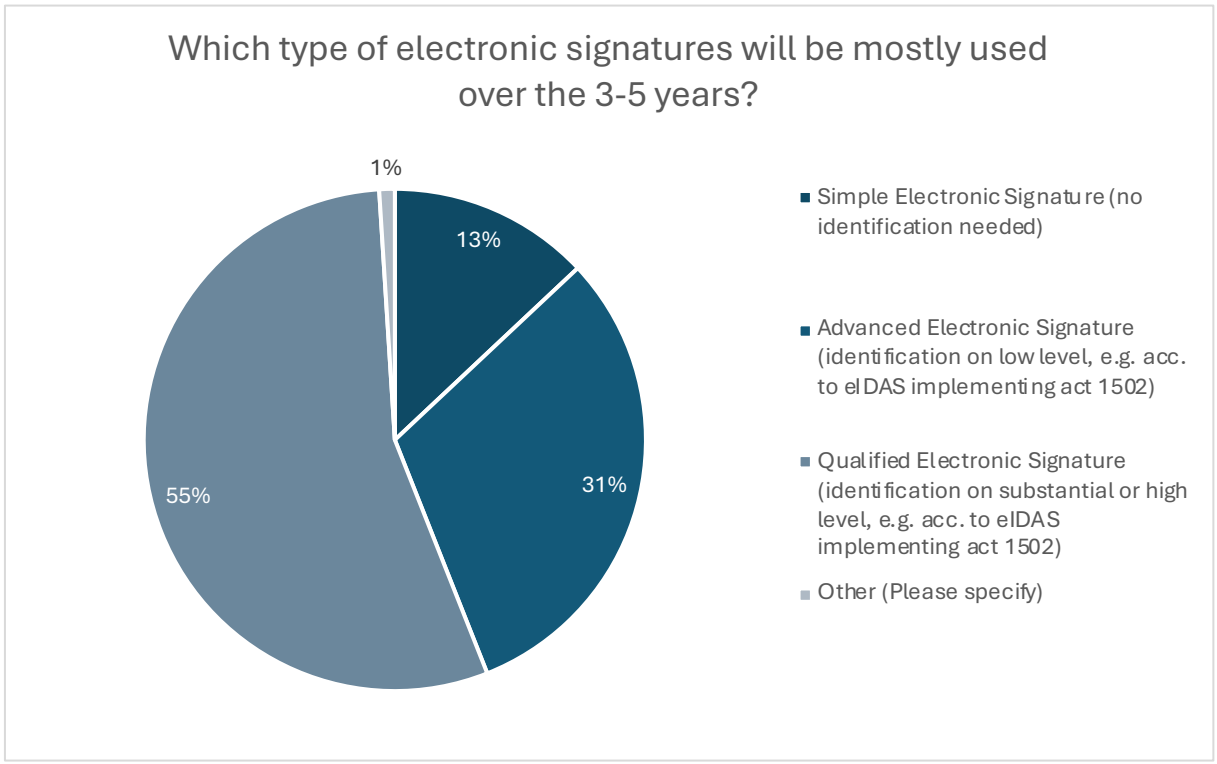
Respondents identified B2B as the key growth area for the use of electronic signatures, with 37% of responses, followed closely by B2C with 36%. There is also a noticeable increase in the adoption of e-signatures in the public sector (22%).



In terms of sectors expected to see the highest usage of electronic signatures, the financial services sector leads with 77%, followed by the public sector (62%) and healthcare (49%). The telecommunications and internet sector, as well as e-commerce and retail, will also gain importance, albeit to a lesser extent.



Regarding types of signatures, 55% of respondents anticipate an increasing popularity of qualified electronic signatures. Participants also expect that the prices of electronic signatures are likely to decrease, as indicated by 20% of respondents who predict a moderate price drop.



However, significant barriers to the wider adoption of electronic signatures include poor user experience (67%) and the lack of global acceptance (55%).

The general outcome of the research is that the future of electronic signatures is marked by innovative trends and growing adoption across various sectors, driven by the anticipated integration with digital wallets and remote signing services. Financial services, healthcare, and the public sector are expected to be the primary users, highlighting a shift towards more secure and efficient digital operations. Despite the optimism, challenges such as poor user experience and lack of global acceptance could hinder broader adoption. However, the developments in the European Digital Identity Framework are seen as potential global standards that could foster greater interoperability and usability in the electronic signature market. Overall, the survey underscores a dynamic market poised for significant evolution but facing crucial hurdles that need addressing.

4.2. The European Digital Identity Framework – a blueprint for global eID and trust services standards?

The European Digital Identity Framework provides a standardized framework for electronic identification and trust services, including electronic signatures, electronic seals, time stamps, registered delivery services and the provision of electronic attestation of attributes. This framework increases the trustworthiness and security of electronic transactions.

eIDAS ensures that electronic identifications and trust services are recognized across all EU member states. This mutual recognition is essential for businesses operating in multiple EU countries, allowing them to use electronic identification and trust services seamlessly across borders.

By enabling legally binding and secure electronic transactions, eIDAS helps businesses reduce administrative burdens and transaction times. This leads to cost savings and improved operational efficiency. It also establishes clear legal rules for electronic transactions, creating a secure legal environment that minimizes risks for businesses.

By simplifying and fostering secure digital transactions, eIDAS supports the EU's Digital Single Market strategy, which aims to extend the benefits of the single market into the digital space. This regulation also promotes digital inclusion by making electronic trust services more accessible and affordable, particularly for small and medium-sized enterprises (SMEs).

eIDAS encourages innovation by setting new standards for electronic trust services and fostering competition, allowing multiple service providers to operate under the same regulatory conditions. For consumers, it enhances trust in digital services by ensuring safer electronic transactions, leading to higher engagement and transaction volumes that benefit businesses.

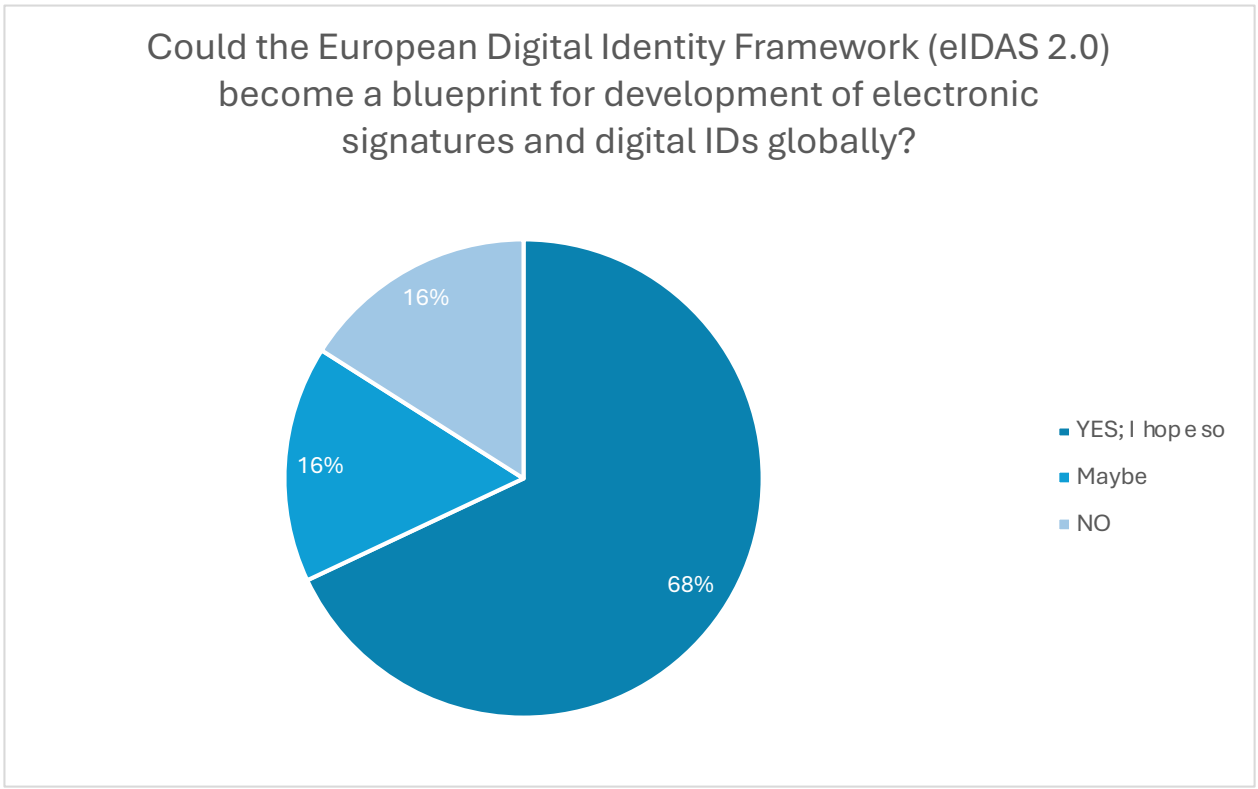
The EUDI Wallet and cloud-based (remote) signatures could accelerate the digitization of both the public and private sectors, enabling more efficient and secure digital services. Digital identity wallets are already emerging globally as a convenient tool for citizen and business identification. The concept of a qualified electronic signature based on the wallet, as outlined in the amended eIDAS regulation, has the potential to become a model for a convenient and, most importantly, mass trust service allowing for remote declarations of intent. The standards introduced by the new European regulation could serve as a global benchmark for the future of digital identification and trust services.

The potential of the new framework as a global blueprint was also confirmed by the respondents of the online survey conducted for this report. The survey gathered insights from market players at the expert level from Europe, Asia, America, and Africa.

Most respondents see the European Digital Identity Framework as a strong candidate for a global standard in electronic signatures and digital identities, citing its interoperability and influence on regions like the U.S., Japan, and Latin America. Some mention the “Brussels effect” as a driver of adoption.

However, challenges remain, including regulatory complexity, legal and cultural differences, and the need for greater openness. Its global success may depend on simplification, interoperability, and strategic promotion, with adoption likely starting in English-speaking countries before expanding further.

The chart below presents the responses in a quantitative manner. They have been appropriately generalized for presentation purposes.



Apart from the quantitative responses, 24 out of 100 participants shared further thoughts about their opinion on eIDAS becoming a blueprint globally. The responses varied, ranging from positive expectations and legal considerations to concerns about the e-signature market. A main finding was that the future of the global electronic signature market depends on technical and legal interoperability, as well as regulatory adaptation to evolving business needs. Greater involvement of public administrations and streamlined adoption in the private sector are essential. The lack of global standards hinders unified implementation, according to the responders.

Current regulations, particularly in Europe, are perceived as overly complex, while the global market develops independently. The growing adoption of Qualified Electronic Signatures (QES) by major companies like Adobe and DocuSign is a key driver. At the same time, QSCD requirements should be simplified, and security measures enhanced to prevent fraud.

Looking at practical examples, it is noticeable that various countries worldwide are already showing interest in the

adapting the principles and standards of the European regulation:

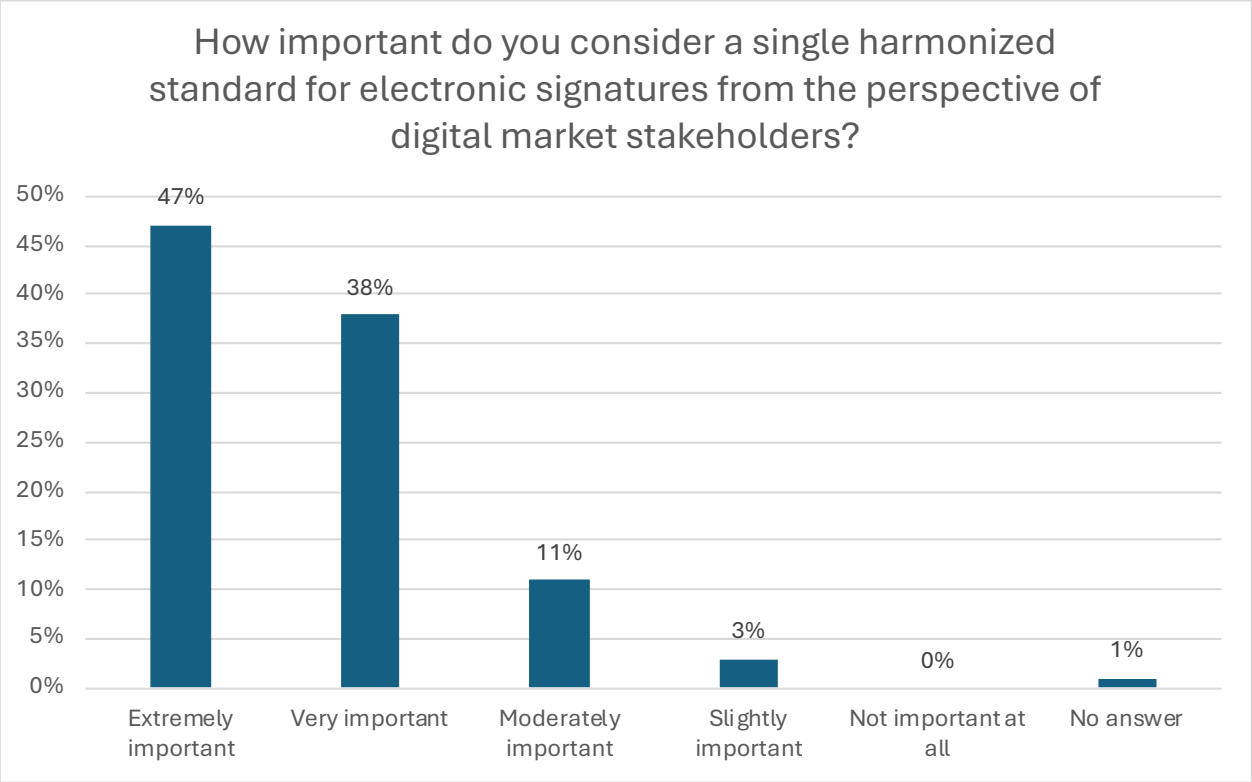
- **USA** – While the United States follows its own regulatory path, some American companies (e.g., Adobe Sign) are implementing Cloud Signature Consortium standards.
- **South America, Africa, and Asia** – Many countries are analyzing the European model to adapt it to their regulations.
- **Canada and Australia** – Their models are more liberal and based on private sector cooperation, which may influence eID standard implementation.
- **Japan** – Exploring various approaches to digital signature implementation, though regulatory and technological differences hinder system harmonization.

To conclude, the establishment of the European Digital Identity Framework could serve as a reference point for other world regions. However, adopting this model requires adaptation to local legal systems and identity management approaches. Countries with strong state oversight over digital identity (e.g., in Europe) may find it easier to implement similar solutions, whereas nations with more decentralized systems (e.g., the USA) may face greater challenges. In the long term, the amended eIDAS could become a foundation for global regulations on e-identification and trust services, but its worldwide success will depend on key markets outside Europe embracing and adapting its standards.

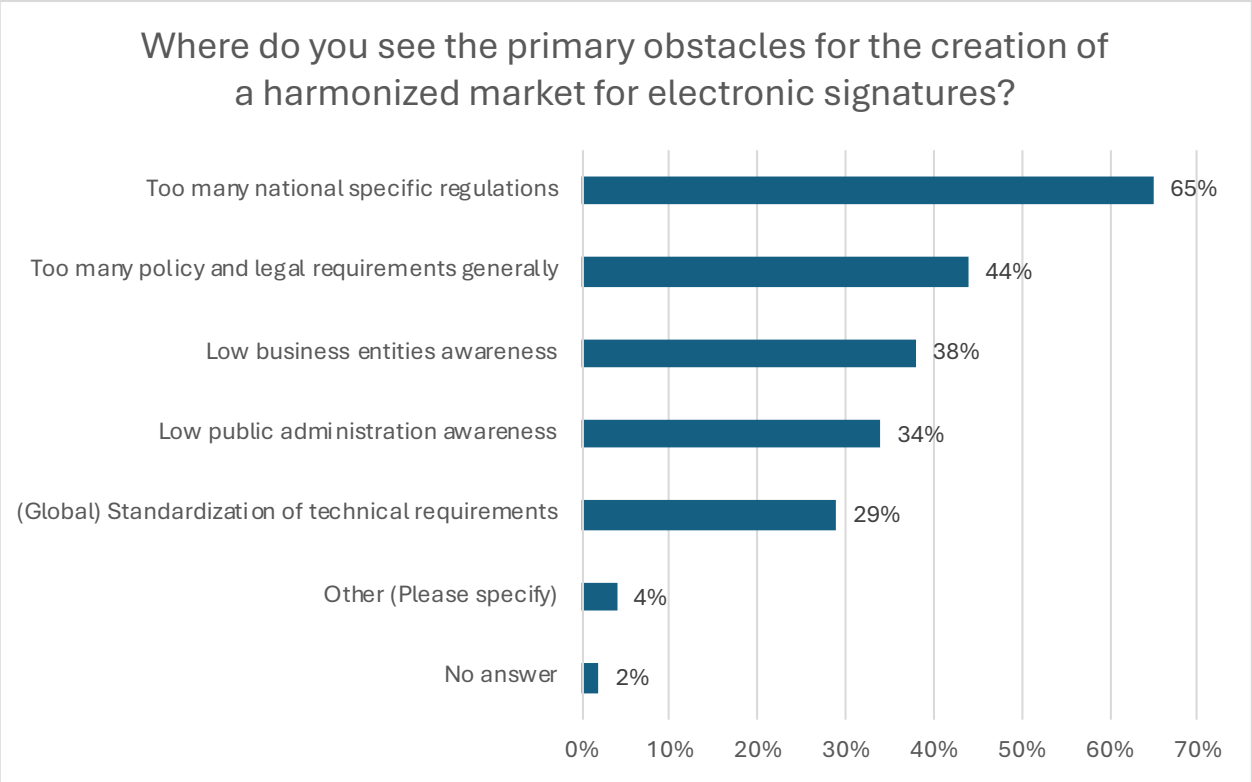
4.3. New landscape of the trust service - review of possible changes in the business and technical standards of the qualified signature usage in business and public administration processes

This chapter is based on the conclusions drawn from the conducted online survey (Present and future of the European and Global Remote Signature market), which provides valuable insights into the current challenges and potential directions for the development of trust services, highlighting the obstacles to creating a harmonized market and the importance of unified standards for stakeholders.

Data regarding the importance of a unified, harmonized standard for electronic signatures from the perspective of digital market stakeholders indicates strong support for this issue. A significant 85% of respondents believe that such a standard is either extremely important (47%) or very important (38%). Only 11% of respondents view this matter as moderately important, while just 3% consider it slightly important. Notably, no one deemed the harmonized standard completely unimportant, underscoring a strong belief that such a standard is crucial for the functioning of the digital market.



The most frequently mentioned barrier, cited by 65% of the respondents, was the high number of country-specific regulations. Another significant obstacle is excessive policy and legal requirements, mentioned by 44% of respondents. A lack of awareness among businesses was identified by 38% of participants, while insufficient awareness in public administration was noted by 34%. Global standardization of technical requirements was considered a challenge by 29% of respondents.



The high level of support for a harmonized standard emphasizes that stakeholders recognize its potential to increase trust and efficiency in electronic transactions, as well as to simplify compliance with regulations across different jurisdictions, making it easier for businesses to operate in the digital marketplace.

CONCLUSIONS

Electronic signatures—particularly cloud-based signatures—are poised to become a global mass service for both businesses and individual users. Businesses will increasingly rely on them to facilitate international trade and regulatory recognition, while individual users will benefit from their integration into mobile identity wallets and remote identification tools. For both groups, a key driver for adopting qualified e-signatures is their role in ensuring cybersecurity and legal validity in digital transactions.

Navigating evolving regulations, technological standards, and shifting customer expectations presents a significant challenge for individual providers. The Cloud Signature Consortium unites industry leaders, technology developers, and trust service providers to address these complexities through collaboration. By establishing harmonized standards, the consortium fosters modularity, flexibility, and adaptability to legal changes, enabling providers to operate seamlessly across global markets while remaining technologically relevant and compliant with diverse regional frameworks. This approach benefits local signature providers, identity wallet solution developers, and businesses involved in issuing, accepting, and recognizing electronic signatures.

A deeper analysis of future business models should include mapping the roles and rights of organizations in certificates for remote signatures. Even for one-time-use signatures, establishing a clear framework for proving authorization and authority enhances trust and usability.

This report has highlighted the diverse global landscape of signature solutions. Despite the coexistence of multiple legal and technical frameworks, the electronic signature market is highly mature in most regions. The adoption of common standards has already enabled a degree of interoperability, and a clear shift toward cloud-based signatures is evident. This approach is widely regarded as the state-of-the-art method for delivering secure and efficient digital signing solutions. Research findings, surveys, and expert interviews all indicate that a unified standard would accelerate market growth, making services more accessible to users, expanding opportunities for providers, and enhancing security, liability, and interoperability worldwide. In this evolving landscape, the Cloud Signature Consortium plays a crucial role in shaping the present and future of the electronic signature industry.

METHODOLOGY

This report was developed based on a complex research methodology, including various approaches – qualitative and quantitative. To provide a comprehensive picture and high-quality results, the following methods were used: Mystery shopping, Individual In-Depth Interview, Computer Assisted Web Interview – Online Survey, Desk Research. Additionally, the report was also enriched with expert knowledge, which expands the scope with a specialist perspective.

Individual In-Depth Interview (IDI)

Ten individual in-depth interviews were conducted with representatives of institutions dealing with trust services around the world. The interviews took place in January and February 2025 and their purpose was to:

- Understand the challenges and opportunities related to the implementation of trust services,
- Assess the impact of legal frameworks such as European Digital Identity Framework on the activities of global stakeholders,
- Identify key technological and market trends.

The IDIs provided valuable analytical material based on the experience of experts and practitioners in the industry and gave a picture of their approach to regulation and future plans or market trends.

Online Survey

The online survey, entitled Present and Future of the European and Global Remote Signature Market, was conducted between December 2024 and February 2025. The survey targeted key stakeholders in the digital signature ecosystem, including trust service providers, technology companies, regulators and organizations using digital signatures. The survey included several questions regarding:

- Legal framework, including the European Digital Identity Framework (eIDAS 2.0),
- Availability, integration and use of remote signatures,
- Market dynamics and trends,
- Customer expectations.

The results provided important quantitative data that allowed us to identify current trends and key factors influencing the development of the digital signature market. In the course of the research, 100 surveys were completed by respondents.

Mystery shopping

The mystery shopping study aimed to evaluate 6 products offered by various trust service providers. The study was conducted in January 2025 and included an analysis of such aspects as:

- The process of purchasing and activating services,
- Customer service,
- Compliance with legal requirements,
- Quality and usability of the offered solutions.

Desk research

The analysis of source materials, industry reports, legal acts and scientific articles was an important complement to the data collected during the empirical research. As part of the desk research, best practices and main directions of development in the field of remote signatures were also identified.

Expert Knowledge

The report included the substantive input of experts (from Obserwatorium.biz and Nimbus) in the field of digital technologies, remote signatures and legal regulations. The experts provided a unique perspective, enriching the analysis with recommendations and data interpretations.

ANNEX
- ONLINE SURVEY -
QUESTIONNAIRE

Present and future of the European and Global Remote Signature market - online survey

Fields marked with * are mandatory.

CLOUD SIGNATURE CONSORTIUM

Thank you for taking the time to participate in our online survey “Present and future of the European and Global Remote Signature market”.

The goal of this survey is to better understand key issues related to the current market landscape and its potential, focusing on legal frameworks (particularly the European Digital Identity Framework), market dynamics, and customer trends.

This survey is targeted at relevant market stakeholders, including:

- Trust Service Providers issuing digital certificates for electronic signatures
- Identity Providers
- Identity Proofing Providers
- Digital Wallet Providers
- eID Hubs
- Signature Platform Providers

About the Author

This survey is being conducted by Obserwatorium.biz and NIMBUS, for a study commissioned by the Clo ud Signature Consortium (CSC). CSC is a global nonprofit association consisting of industry and academic organizations dedicated to developing open standards for cloud-based digital trust services and promoting worldwide interoperability. Learn more about CSC at cloudsignatureconsortium.org.

OBSERWATORIUM.BIZ NIMBUS

The data collected will be analysed to produce statistical insights and compiled into a concise study, which will be publicly released in 2025. Please rest assured that neither your name nor your organization's name will be disclosed.

Data Protection

Participation in this survey does not require your or your company's name. No registration is necessary. After submitting your responses, you will have the option to save them as a PDF.

In accordance with applicable data protection laws, you are able to submit your responses anonymously. If you have any questions or wish to exercise your rights regarding data access or deletion, please read the E U Survey privacy statement (https://ec.europa.eu/eusurvey/home/privacystatement) or contact our data protection officer at kontakt@obserwatorium.biz.

Thank you for your valuable input!

For those who complete this survey and submit their email at the end, we will send a report containing the research results before its publication date.

PRESENT AND FUTURE OF THE EUROPEAN AND GLOBAL REMOTE SIGNATURE MARKET - ONLINE SURVEY

* 1. Which type of provider are you?
(Please select every option that is proper for your company)

- ◯ Qualified Trust Service Provider
- ◯ Trust Service Provider
- ◯ Identity Provider
- ◯ Identity Proofing Provider
- ◯ Wallet Provider
- ◯ Signature platform provider

Other (Please specify)

* 2. What is the size of your company?

- ◯ micro enterprise (up to 9 employees)
- ◯ small (10-100 employees)
- ◯ medium (101-1000 employees)
- ◯ big enterprise (+1000 employees)

* 3. In which region are you mainly active?
(Please select every option that is proper for your company)

- ◯ South-East Asia (Thailand, Vietnam, Malesia…)
- ◯ Central Asia (Kazakhstan, Uzbekistan, Iran…)
- ◯ Middle East (Saudi Arabia, UAE, Bahrain…)
- ◯ China
- ◯ India and Pakistan
- ◯ Japan
- ◯ South America
- ◯ North America
- ◯ Australia and Oceania
- ◯ Africa
- ◯ Europe - non-EU
- ◯ Europe - EU

* 4. What is your role in electronic signature solutions industry?
(Please select every option that is proper for your company)

- ◯ Certificate authority
- ◯ Remote signature creation device provider
- ◯ Remote qualified signature service provider (long term certificates)
- ◯ Remote qualified signature service provider (short term certificates)
- ◯ Online Signature Creation - Workflow provider
- ◯ Identity proofing provider for remote signatures

Other (Please specify)

* 5. Has your company implemented the Cloud Signature Consortium API?

- ○ Already implemented
- ○ Not yet, but planning to
- ○ No, not interested
- Other (Please specify)

6. If already implemented - what was your motivation to integrate the API?

7. If not implemented what are the reasons for it?

* 8. What key product developments do you predict for electronic signatures over the next 3–5 years?
Maximum 2 selection(s)

- ○ Remote services for electronic signing (applications or other cloud solutions that allow customer to sign documents without hardware-based solutions)
- ○ Remote onboarding to electronic signature (solutions which enable to issuing of electronic signature certificates without the necessity of the physical presence in the office, with the advisor etc.)
- ○ Platform-integrated electronic signatures (signing process embedded in the business process like signing agreement within electronic banking system or within dedicated signing platform)
- ○ Issuance of hardware-based certificates (like smart card, USB-key, SAM via Global Platform) Signing via the wallet (signing process integrated in ID wallet solution)

Other (Please specify)

* 9. In which area do you see use of electronic sigantures increasing the most over the next 3-5 years?

- ○ Increase of electronic signature usage in business to consumer relations (B2C)
- ○ Increase of electronic signature usage in business to business relations (B2B)
- ○ Increase of electronic signature usage in public administration
- ○ No answer

Other (Please specify)

* 10. In which sectors will electronic signatures be used the most in next 3-5 years?
Maximum 3 selection(s)

- ○ Consumer Goods
- ○ E-Commerce and Retail
- ○ Energy + Environment
- ○ Telecom + Internet
- ○ Transportation and Logistics
- ○ Travel + Tourism
- ○ Financial services
- ○ Health
- ○ Public Sector

Other (Please specify)

* 11. Which type of electronic signatures will be mostly used over the 3-5 years?

- ○ Simple Electronic Signature (no identification needed)
- ○ Advanced Electronic Signature (identification on low level, e.g. acc. to eIDAS implementing act 1502)
- ○ Qualified Electronic Signature (identification on substantial or high level, e.g. acc. to eIDAS implementing act 1502)

Other (Please specify)

* 12. The final price for the customers of electronic signatures over the next 3-5 years will decrease/incerese /not change.

- ○ 5 - Strong Increase
- ○ 4 - Considerable Increase
- ○ 3 - Moderate to Considerable Increase
- ○ 2 - Moderate Increase
- ○ 1 - Slight Increase
- ○ 0 - Neutral (will not change)
- ○ -1 - Slight Decrease
- ○ -2 - Moderate Decrease
- ○ -3 - Moderate to Considerable Decrease
- ○ -4 - Considerable Decrease
- ○ -5 - Strong Decrease

* 13. How important do you consider a single harmonized standard for electronic signatures from the perspective of digital market stakeholders?

- ○ Extremely important
- ○ Very important
- ○ Moderately important
- ○ Slightly important
- ○ Not important at all
- ○ No answer

* 14. Where do you see the primary obstacles for the creation of a harmonized market for electronic signatures? Maximum 3 selection(s)

- ○ Too many policy and legal requirements generally
- ○ Too many national specific regulations
- ○ (Global) Standardization of technical requirements
- ○ Low public administration awareness
- ○ Low business entities awareness
- ○ No answer

Other (Please specify)

* 15. What are the key obstacles to wider adoption of electronic signatures? Maximum 3 selection(s)

- ○ Lack of global acceptance of electronic signatures
- ○ Weak user experience
- ○ To little use cases
- ○ To high pricing
- ○ No answer
- ○ Other (Please specify)

* 16. What is the most likely scenario regarding the global market for electronic signatures in the next 3 -5 years?

- ○ The global market will transform into a more unified ecosystem due to eIDAS implementation and standardization processes. Other markets will follow the model.
- ○ The global market will fragmentize into many local markets with specific technical and legal rules with decreasing interoperability
- ○ The global market will not change a lot regarding interoperability
- ○ No answer

Other (Please specify)

* 17. Could the European Digital Identity Framework (eIDAS 2.0) become a blueprint for development of electronic signatures and digital IDs globally?

18. Do you have any other remarks regarding the future global development of the electronic signature market?

Thank you!

Please leave your email if you want to get a report containing the research results before its publication date.

CLOUD SIGNATURE CONSORTIUM

CLOUD SIGNATURE MARKET

EU & GLOBAL PERSPECTIVE

INDUSTRY MARKET REPORT 2025

CONTACT

Cloud Signature Consortium vzw
Rue de Spa 28 | BE 1000 Brussels
https://cloudsignatureconsortium.org
info@cloudsignatureconsortium.org