OBSERWATORIUM . BIZ
ISBN 978-83-954468-0-1

PAPERLESS BUSINESS

Commercialisation of eID and Trust Services in Poland and Europe

SPECIAL REPORT

main patron: EFPE
scientific partner: C@ntrum Prawnych Problemów Techniki i Nowych Technologii
social partner: Polska 5.0
partner: KIR
partner: asseco DATA SYSTEMS
partner: SIGNICAT
partner: go.eIDAS
honorary patron: PIIT
honorary patron: Ministerstwo Przedsiębiorczości i Technologii

Dear Readers,

as the authors of the "PAPERLESS BUSINESS – The Commercialisation of eID and Trust Services in Poland and Europe" report, we would like to express our gratitude to all the Institutions and Individuals who contributed to the creation of this document. It is our third publications on this important area of digital economy released over the last two years.

First of all, we would like to thank the European Forum on Electronic Signature and Trust Services, which is the Main Patron of the Report, the Honorary Patrons – the Ministry of Entrepreneurship and Technology and the Polish Chamber of Information Technology and Telecommunications, the Partners of the Report – Asseco Data Systems SA, Krajowa Izba Rozliczeniowa SA, SIGNICAT, go.eIDAS, and finally, our Public Patron – Fundacja Polska 5.0.

We would like to thank the representatives of commercial institutions active in the digital economy market, the representatives of public administration, and the independent market experts who agreed to support our project with their valuable statements and opinions, which we have included in the Report.

We hope that the Report will give you a clearer picture of the specificity and present condition of the Polish electronic identification (eID) and trust services market, especially when compared against the main trends of the European market. Effective implementation of solutions such as cloud-based electronic signature, electronic seal, or electronic delivery may spearhead a true breakthrough on the online services market and, combined with the emerging electronic identification market in Poland, determine the next step in secure and effective digitisation of the relationship between citizens, consumers, entrepreneurs, business operators and government administration in Poland.

Enjoy reading the report!

Obserwatorium.biz Sp. z o.o

PODZIĘKOWANIE

OBSERWATORIUM . BIZ

BASIC CONCLUSIONS OF THE REPORT – PRESENTED IN FAQ FORMAT

WHAT ARE THE BENEFITS OF THE DEVELOPMENT AND POPULARIZATION OF ELECTRONIC IDENTIFICATION (eID) AND TRUST SERVICES?

Conclusion of contracts (even the simplest ones) and contract-related payments are one of the building blocks of the economy. The digitalisation of the Polish economy in respect to these areas is unbalanced. Electronic payments via cards, applications or smartphones are commonplace by now. Concluding a contract requires a trip to a given institution, which is time-consuming and does not fit in well with the needs of modern-day reality. Electronic ID tools and trust services address these needs, closing a serious gap in the digitalisation of the Polish economy and society.

WHAT IS SHOWN ON THE MAP OF POLISH eID/TRUST SERVICES?

The map shows several mature trust service providers – mainly electronic signature providers, many of whom offer qualified services. At the same time, more and more operators are developing electronic identification systems, which often integrate multiple identity providers (for instance, banking sector providers). There are also providers of individual trust services, such as signature validation or e-delivery, with ambitions to implement qualified services. Integrators are trying to develop a wider range of services and present the final digital service provider with an ergonomic and standardized solution – similar to the ones offered by payment integrators to online retail outlets..

WHAT TRENDS CAN BE SEEN ON THE EUROPEAN eID AND TRUST SERVICES MARKET?

What we see is a market that is growing in strength – there are nearly 200 qualified service providers, while 17 electronic identification schemes have already been notified. The eIDAS regulation in force ensures standardisation and cross-border compatibility of the solutions. As far as Poland is concerned, we will have to accept the multiplication of foreign tools adapted to our market, at the same time promote our own solutions or even develop our platforms that will be integrated with identity providers (e.g. banks) and digital service providers from other EU countries. We also see a push towards standardization of new tools, such as video verification during onboarding for trust services.

KEY ENABLERS FOR eID AND TRUST SERVICES IN 2020

THE TOOLS:

- developing solutions that meet the expectations of today's end user

  - an identification scheme based on the digital identity systems currently in place (e.g. the ones provided by banks or the government) adequate for the purposes of onboarding or verifying the customer's attributes (such as their age);

  - a qualified electronic signature available online (issued on the basis of video verification, eID, or other means);

  - electronic delivery as an alternative for registered mail, available after convenient onboarding e.g. with eID;

  - electronic signature validation, available for plug&play integration to all digital service providers.

THE DIGITAL SERVICE PROVIDER AND THE USER:

- the service provider (e.g. a telecommunications operator sending a contract to be signed electronically) must obtain a process based on eID and trust services, configured to its needs. Education on the legal and security aspects is key to success in developing a wide "network of acceptance" for trust services;

- the end user does not have to understand the complexity of eID and trust services – they will successfully go through the process if they trust the service provider (e.g. a telecommunications operator)with whom they are signing a contract online, and the process itself, e.g. the process of creating a signature, is just as convenient as an electronic payment at an online shop;

THE MARKET AND THE REGULATOR:

- creating a common space for the development of new tools and uses for eID and trust services: video verification as an onboarding tool for trust services, utilising the identity document in smart phone app (mObywatel)l application and the electronic identity card (the "e-dowód") for commercial use, development of public and commercial electronic deliveries;

- close cooperation between providers of trust service providers/integrators and digital service providers so that the needs of those digital service providers can be understood and the services developed in line with their expectations and the expectation of end users – individual clients and businesses.

TABLE OF CONTENTS

Mobile Electronic Signature

SimplySign

by asseco

- Administration
- Business
- Customers

Free The Power of Electronic Signature

Sign all documents,
regardless of the place and time.

Read more **simplysign.pl** Hotline **+48 91 4801 300**

asseco
DATA SYSTEMS

INTRODUCTION

The "PAPERLESS BUSINESS – Commercialisation of eID and Trust Services in Poland and Europe" report is another one in a series of widely available market reports on electronic identification and trust services produced by Obserwatorium.biz. In 2017 two dedicated reports were developed: "eID Report – Electronic Identification in Poland" and "Breakthrough in On-line Services – Development of Trust Services in Poland". Both documents formed a kind of a basic compendium of knowledge about this emerging market, explaining the basic terms, presenting the first applications in Poland and examining the issue in an international context. The reports showed that eID and trust services can be beneficial both in government administration, where remote identification of citizens and entrepreneurs was (and still is) a pathway towards effective delivery of e-services by the state, and in the commercial realm, where effective processes of customer onboarding or obtaining a client's binding signature on a contract in a remote transaction are vital.

The eIDAS Regulation, The eIDAS regulation that entered into force a year before, brought about the establishment of clear regulation of eID and trust services in the Polish legislation (through the implementation of the Act on trust services in 2016 and its subsequent amendment in 2018, which expanded the nomenclature in the Act to include electronic identification), as well as an increased interest in this market among solution providers, digital service providers, the end users themselves, and in particular, businesses. As such, the present report will focus primarily on the practical applications for such services. The first chapter features a map of Polish eID and trust service providers that enables the reader to look up the operators present on the Polish markets and the functions they perform on this market, i.e. current or prospective service providers, service recipients or integrators – interestingly, some operators, such as banks, can fulfil several functions at the same time.

The next chapter demonstrates the development of the regulatory environment and presents the changes in the regulations governing this aspect of the European market and the market itself. This subject is important not only in view of the potential inspiration one can draw from the European solutions, but also due to the direct influence that international specific standards (such as those concerning qualified delivery services or video onboarding for trust services) have on Polish standards and products, as well as the fact that foreign players are increasingly confident about entering the Polish eID/trust service market. The third chapter presents the potential for commercialisation in selected market sectors – it at least initially reveals the sectors of the commercial market (financial, HR, energy, telecommunications and other) where trust services can be effectively used and estimates the value of this market.

The last chapter presents market development scenarios and describes the main aspects and problems that will have to be tackled by the market and its participant in order to fully harness the potential of eID and trust services for the successful transformation of the digital economy in Poland.

Chapter 1 -

MAP OF eID AND TRUST SERVICES IN POLAND

1.1 Introduction

There is a large group of providers of electronic identification (eID) solutions and trust services, both Polish and foreign. When offering their products, these providers are trying to convince the market that they are the ones that are able to protect the increasingly large volumes of various electronic transactions while maintaining security and convenience. These services are aimed at citizens, businesses and government administration alike, and their primary benefit lies in eliminating "paper" processes, expediting the processing, and providing greater transparency for all market participants.

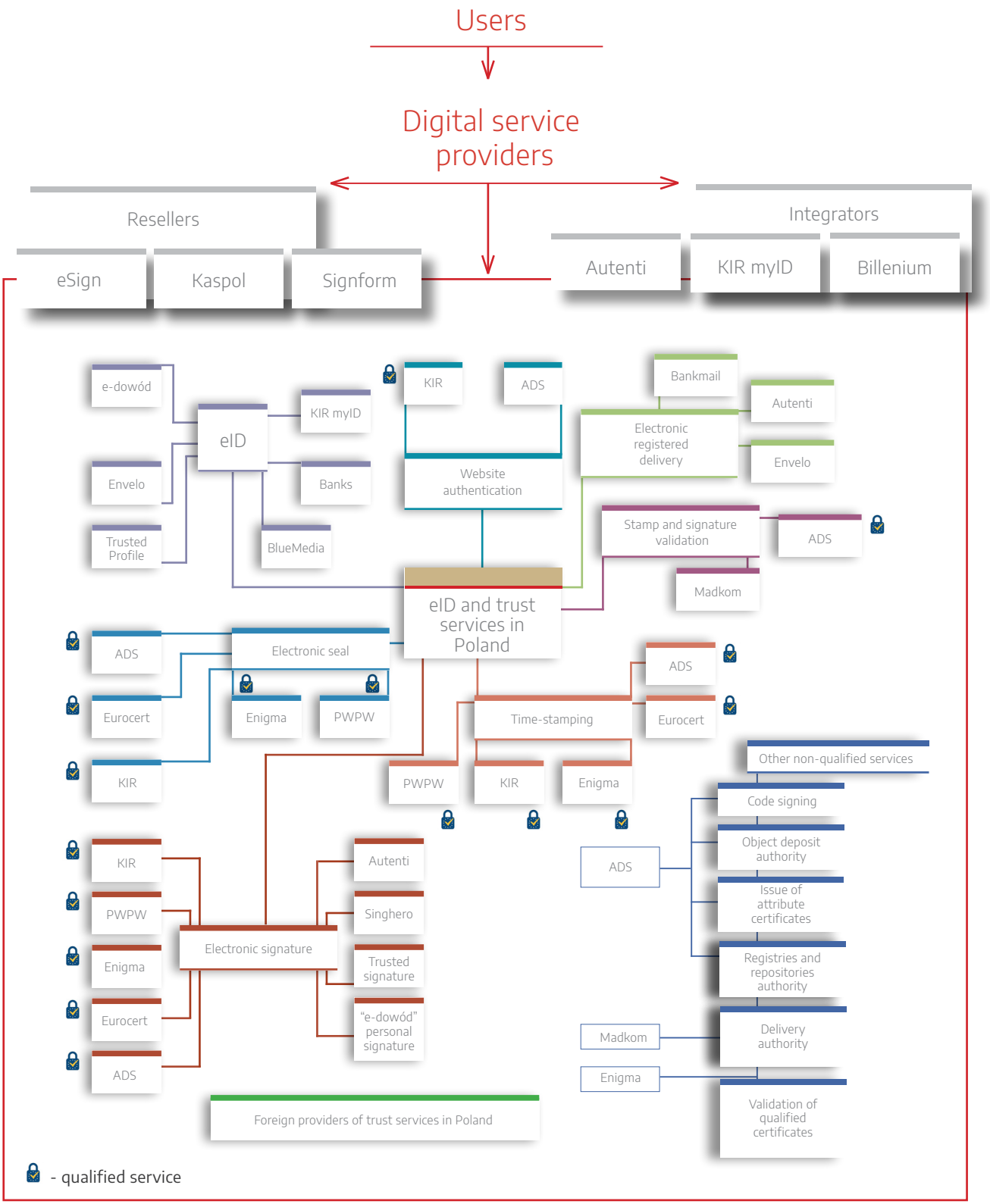
The ambition behind this report is to put forward a map of eID and trust services in Poland as at mid-2019. In the authors' opinion, the domestic market ecosystem can be divided into 5 main groups:

The eIDAS Regulation, which came into force in July 2016, defines the conditions for the functioning of the eID and trust services market in the European Union's single digital market. Since then, the market has been developing under more uniform and standardised rules, but has still yet to enter its rapid growth and the full commercial exploitation of its potential.

- domestic and foreign providers of electronic identification (eID) and trust services
- resellers of electronic identification (eID) and trust services;
- integrators of electronic identification (eID) and trust services;
- digital service providers who incorporate these services into their processes;
- end users – individual consumers or businesses, who are the final recipients of these solutions.

It should be noted that both qualified services offered by qualified suppliers (fully compliant with the eIDAS regulation) and non-qualified services are available on the market. The choice of a qualified or a non-qualified service is determined by the specific use and the extent of applicable regulations governing a given process. Such regulations are not limited to the Act on trust and services and electronic identification, but also include, for example, Telecommunications Law or the Civil Code itself, as appropriate.

MAP OF eID AND TRUST SERVICES IN POLAND

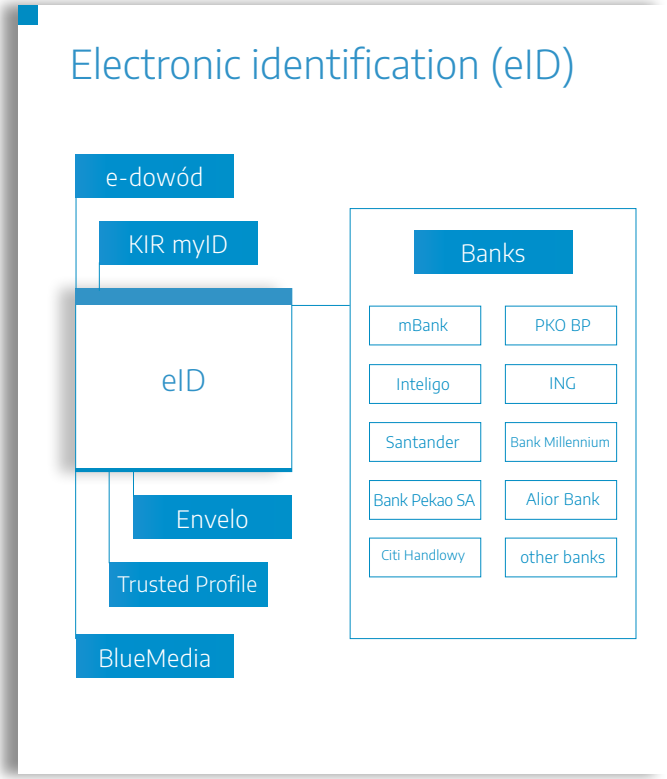


Abbreviations used:
ADS = Asseco Data Systems SA
KIR = Krajowa Izba Rozliczeniowa SA (National Clearing House)
PWPW = Polska Wytwórnia Papierów Wartościowych SA
(Polish Security Printing Works)

1.2 Electronic identification (eID)

Electronic identification services are a necessary prerequisite for the processing of transactions in the digital world in a manner that is secure for both parties. The number of things that we as consumers and citizens can do through electronic channels is continuously increasing. In these cases we act as specific individuals, identifiable by name.

Therefore, during such a process – including opening a bank account online, arranging a doctor's appointment via a mobile app, or filing a tax return – it is crucial for both parties of the arrangement that the applicant is identified in a proper, secure and ergonomic manner.



There are many electronic identification means in Poland that enable the use of electronic identity online: from the latest "e-dowód" solution, through the Trusted Profile and the bank-provided means, to Envelo and myID developed by KIR.

Developing an electronic identification system makes it possible to bring into the digital world the processes which previously required the client to personally visit a service point/government office or meeting a courier in person. For example, the myID service implemented by the National Clearing House (KIR) enables users to remotely confirm their identity based on data from trusted entities defined as identity providers, e.g. banks. By applying authentication mechanisms in online banking, we can achieve the "one-stop-shop" effect – quick, simple, and secure access to commercial and public online services.

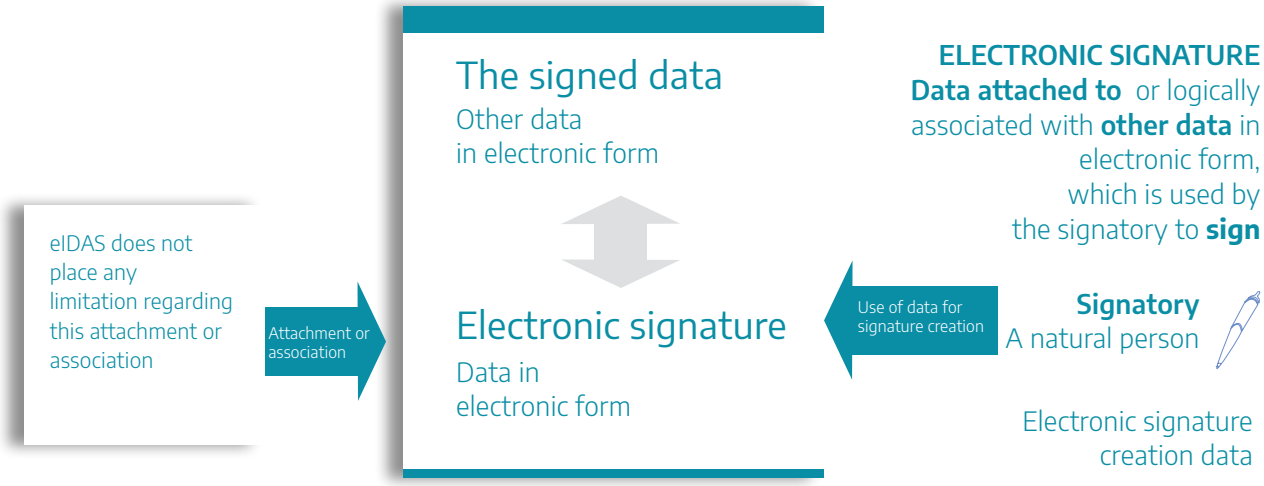
However, in some cases, electronic identification in online processes is insufficient to ensure the security of an online transaction. Achieving full digitisation of all processes – both in the commercial world and government administration – often requires a combination of the two components (eID + trust service).

The potential of electronic identification

Digital identity enables the development of modern remote trust services (e.g. cloud-based electronic signature). Such services require that the issue of a comprehensive remote authentication mechanism be addressed. According to the eIDAS regulation, user registrations for such a service can be performed based on electronic identification with a substantial or high assurance level, provided the initial identity proofing was made directly. When an electronic identification mechanism is used, a user of a qualified service does not have to appear in person at the registration point, and the service can be provided remotely in its entirety. Other trust services requiring prior user registration will also benefit from electronic identification mechanisms.

1.3 Electronic signature service

The electronic signature is, without a doubt, the most well-known and well-understood trust service. It is worth noting, however, that is there are currently several types of electronic signature available on the market: qualified, advanced and simple.



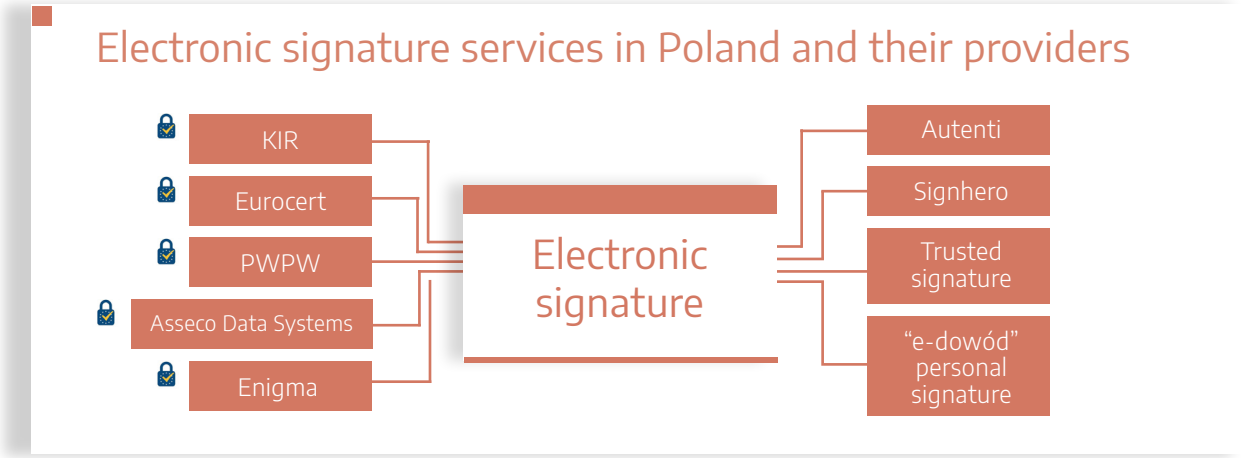
Concluding distance contracts via electronic means of communication has been permitted for several years both in Polish and EU legislation. In many cases, distance contracts can be concluded with just a simple electronic signature, i.e. one that is neither advanced nor qualified. An electronic signature "means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign." eIDAS does not place any restrictions on the technology used for such attachment or association.

In technical terms, there is no difference between an advanced electronic signature and a qualified one. A qualified electronic signature is an advanced electronic signature, with the key distinction of being created by a qualified electronic signature creation device and verified by a qualified certificate. A qualified electronic signature has the equivalent effect of a handwritten signature throughout the European Union.

QUALIFIED ELECTRONIC SIGNATURE = HANDWRITTEN SIGNATURE

An electronic signature can be used as admissible evidence in legal proceedings, even if it is not advanced or qualified. However, the court is not required to verify the source of the signature in the case of qualified electronic signatures.

In terms of qualified signatures, there are cloud-based solutions available on the market (the keys are stored by a qualified entity), as well as solutions supporting traditional signatures created with card readers and cryptographic cards.



The trusted signature is dedicated to holders of a trusted profile who wish to sign motions and applications submitted to public entities.

On the other hand, the electronic signature solution referred to as the 'personal signature' (podpis osobisty), is an advanced signature. In interactions with public entities, the personal signature will have the same effect as a handwritten one. The above will also apply to non-public entities if both parties give their consent. The available providers of online platforms (Autenti, Signhero) offer online services for creating signatures and pre-assessing their evidentiary value. Simple signatures are used in this case. According to the data aggregated by the Ministry of Digitization and supplied by qualified trust service providers since early May 2019, there were nearly 565 thousand active qualified certificates in Poland.

The concept of cloud-based signatures has the potential to revolutionize the way electronic signatures are used and popularize the e-signature service, especially among individual consumers. One advantage of cloud-based signatures is that they eliminate the need to have a reader or token. Another is that the signatures are shared via remote identification. A qualified e-signature service in the cloud can be expanded to include additional functionalities, such as an electronic time stamp.

The use of an electronic signature is compulsory for:

- signing financial statements by companies
- VAT reporting with a Standard Audit File for Tax (SAF-T)

Qualified electronic signatures are used for:

- sending forms to the KIO (the National Board of Appeal),
- lodging procedural documents with courts for writ of payment proceedings,
- electronic communication with the Social Insurance Institution (ZUS), e.g. signing applications for certificates on the absence of arrears in payments of social security contributions, signing declarations,
- obtaining electronic extracts for all entities registered in the National Court Register (the KRS) (pdi.cors.gov.pl),
- signing official correspondence with government administration bodies via the electronic inbox,
- issuing invoices in electronic form,
- participating in electronic tenders and auctions (e.g. www.e-przetarg.pl),
- signing reports to the General Inspector of Financial Information (GIIF),
- electronic reporting of personal data files to tPresident of the Personal Data Protection Office (UODO),
- filing e-declarations with the Insurance Guarantee Fund (UFG),
- all matters where written declarations of will are required by law (e.g. leasing agreements, consumer loan agreements, copyright transfer statements).

Simple electronic signatures are used for:

- contracts with customers
- specific-task contracts, contracts of mandate
- employee applications
- acceptance protocols
- rental contracts
- confidentiality agreements

REPORT EXPERT

Robert Trętowski
Vice-President of the Board, KIR

The electronic signature (both qualified and non-qualified) is gaining popularity and will continue to do so as more opportunities for use become available, and as electronic signatures become mandatory for specific operations. The requirement to submit financial statements in electronic format with a qualified signature is just the most recent example.

Nowadays, the potential applications of e-signatures are not limited to business, but extend to private users as well. A survey conducted by Kantar TNS for the Polish Bank Association and KIR showed that a significant 74 percent of respondents would like to digitally sign telecommunications services contracts, 62 percent would like to do the same with banking services contracts, 57 percent – utility service contracts, 51 percent – insurance services contracts, and 50 percent – medical services contracts We therefore see great promise in a service we are currently developing – mSzafir:
a qualified, cloud-based electronic signature.

Secure and convenient identity proofing is an issue of key importance for the further development of digital services – both in the government administration and the commercial sphere. As long-time providers of an infrastructure for secure digital exchange of sensitive information, we actively participate in this process, developing products that respond to market demand. The myID service, which enables remote identity proofing in accordance with the highest security standards, is one example.

Both mSzafir and myID are solutions aimed at supporting the implementation of solutions that push the digitisation of economy forward.

1.4 Electronic seal service

The next service is the electronic seal, which is used to seal documents, data and electronic correspondence. An electronic seal works basically the same as an electronic signature, however:

- Seals are used by legal entities, companies, public agencies, and organisations
- A seal of an organisation is not its signature, and is therefore not used to establish representation or make statements of will on behalf of the organisation
- Seals are used to authenticate documents — proving that the document bearing the seal was issued by the relevant organisation

The service guarantees data integrity, identifies the entity creating the document, and adds an element of non-repudiation recognised by law. Electronically sealed documents are more secure than their paper counterparts, as any modification to the document is automatically detected.

Most seals available on the market are qualified seals (PWPW, Asseco Data Systems , Enigma, KIR, Eurocert), which are fully legally binding and admissible as evidence by law.

Just as with the electronic signature service, the market offers cloud-based (online) seal solutions, as well as traditional solutions utilising a reader and cryptographic card.

The electronic seal allows electronic processes to be automated, especially when used for:

- Banking documents and confirmations of transactions
- Electronic invoices
- Automatic confirmations of transactions in online services
- Automatically issued official (government) certificates
- Securing documentation signed via an IT system – e.g. a confirmation filed with a trusted profile
- Issuing electronic tickets that can be authenticated by anyone

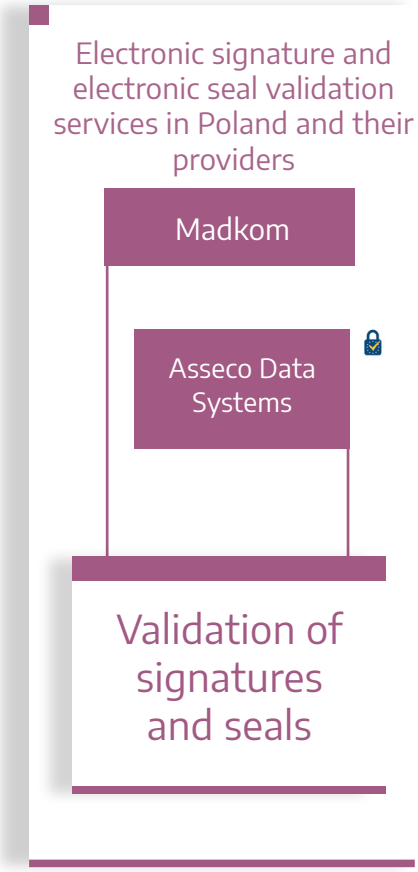
Electronic seal services in Poland and their providers

1.5 Electronic signature and electronic seal validation service

Validation means the process of verifying and confirming that an electronic signature or a seal is valid.
There is a single qualified validation service for qualified electronic signatures and seals available on the Polish market, which is provided by Asseco Data Systems. There is also a provider offering a non-qualified service (Madkom).

In qualified services, the validation process is completed when a certificate of validation is issued. This certificate is admissible as evidence and can be used to settle court disputes. The validation service guarantees accurate validation of a signature or a seal while eliminating the need to verify it personally.

Wherever the risk of inaccurate verification may compromise the security of transactions, e.g. in the case of valuable contracts for large sums, long-term liabilities or tenders for public procurement contracts, the use of validation is essential and guarantees security for the entity accepting signed or sealed documents.



Use of the validation service:

- receiving high-risk declarations and undertakings
- public procurement proceedings
- long-term or financial commitments
- no signature verification tools on the side of the relying party

A validation service may be provided in various forms, depending on customer preference:

- Access via web browser
- Access via API integration
- Access via a dedicated server
- Mailbox validation

1.6 Time-stamping service

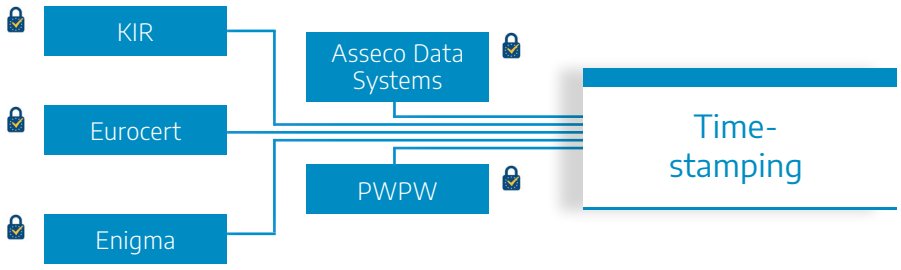
Both qualified and non-qualified time-stamping services are available on the Polish market. The service is aimed towards all those who wish to have proof that an e-document existed at the time of the stamping, or additional secure confirmation of the time of qualified signature creation. In both versions of the service, a reliable time stamp is provided by a trusted third party.

The distinguishing feature of a qualified time stamp is that it produces legal effects of a certain date. Qualified time-stamping can be carried out only by a qualified trust service provider, and the court considers time-stamping to be reliable evidence.

Time-stamping is used wherever the time of the transaction and document creation must be reliably established.

At present, there are several operators of qualified time-stamping services on the market (Asseco Data Systems PWPW, Enigma, KIR, EuroCert).

Time-stamping services in Poland and their providers



Time stamps are used for:

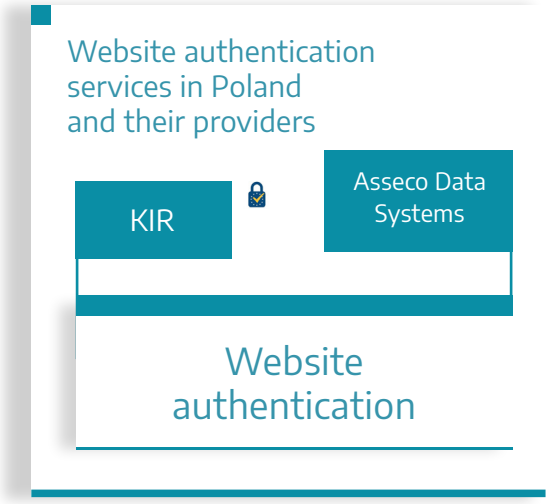
- contracts (bank contracts, insurance contracts)
- invoices
- medical records
- internal electronic documents
- system logs (IT)

1.7 Website authentication service

A certificate for website authentication is a service that provides a certificate that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. This service allows users to set up an encrypted SSL connection between the servers with such certificates, as well as provide secure logging to customers.

In practice, the service works identically to the SSL certificates currently used. The qualified certificate for website authentication establishes legal rules for validating website publishers.

Currently, KIR is the only provider to offer a qualified website authentication service in Poland. Asseco Data Systems is the sole provider of a non-qualified authentication service.

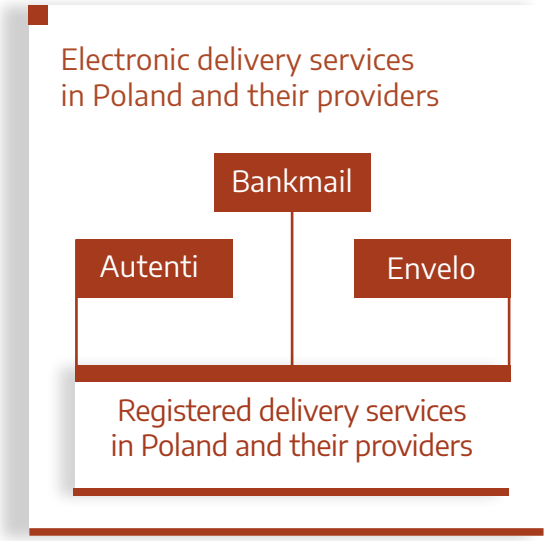


Under the PSD2 Directive, service providers are obliged to use qualified certificates for website authentication – this applies to both banks and payment service providers (Third Party Providers).

1.8 Electronic registered delivery service

Electronic registered delivery service means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

In registered service delivery, a trust service provider operates the service for third parties, provides identification of the sender of the document, the identification of the recipient of the document, ensures the confidentiality and integrity of the document in the process of its transmission, and provides confirmations of sending and receipt.



At present, there are no providers of qualified electronic registered delivery services on the Polish market. The "e-Doręczenie" (eDelivery) project is currently being worked on in the course of legislative and organisational proceedings, and may significantly contribute to digitising delivery services.

However, some companies do provide electronic registered delivery services. At this point in time, we can identify the following electronic mail platforms that issue sending and receipt confirmations and identify senders and recipients:

- **Envelo**
- **Autenti**
- **Bankmail**

REPORT EXPERT

Adam Ptasiewicz
e-Services Officer
Sales Division, Poczta Polska S.A. (Polish mail service)

For trust services to develop, universal availability and effective legal regulations are necessary.

Key changes have been introduced in Poland with the adoption of the Act on trust services (...); we are currently waiting for an act on electronic deliveries. This is of crucial importance in terms of take-up of electronic documents and the availability of such documents for all citizens. Three factors are necessary to ensure faster growth of commercial and public trust services:

- availability of services in the sense of being accessible and easy to use in everyday life
- education to assure potential users that the electronic transfer of documents is secure
- interoperability in terms of compatibility of different systems and ability to exchange and use data

The new public service will no doubt have a positive impact on bringing the benefits of trust services closer to the general public.

1.9 Other supplementary non-qualified services

In addition to the core trust services described above, there are also other trust services available for securing data and processes, namely:

- code signing (Asseco Data Systems)
- object deposits authority (Asseco Data Systems)
- issue of attribute certificate (Asseco Data Systems)
- registries and repositories authority (Asseco Data Systems)
- delivery authority (Madkom)
- validation of qualified certificates (Enigma)

REPORT EXPERT

Mariusz Janczak
Product Manager
Security and Trust Services Division, Asseco Data Systems

The incorporation of full electronic identification into business and administrative processes is a quantum leap in terms of technology and process organisation. Such a system continues to be the missing link in the digital transformation of Polish economy, but there is an increasing number of market signals suggesting that this may soon change.

Electronic identification of natural persons and the functionality of trust services (especially mobile digital signatures) are key legal instruments for the enabling all transactional processes to be conducted in a secure digital world. This system will radically change the relationship between service providers and customers, as well as streamline business processes.

A qualified mobile e-signature available from a smartphone app is a milestone of progress towards stimulating innovation in trust services. By optimising UX on the end-user side the system enables creation of new services, products or business models. This is a key factor to the success of many global ICT companies. Wide take-up of these tools will not only contribute to business growth, but will also significantly improve the ergonomics of the solutions provided by public administration and commercial service providers, such as those from the financial, telecommunications, insurance and medical sectors.

KIR thinks digitally

We focus on development and delivery of innovative solutions, responding to the challenges of technology advancement and legal changes at the national and European level.

We excel in supporting the efficiency of banking and payment sector, e-commerce, and public administration.

We employ our experience and operational maturity to contribute in building a modern, digital economy in Poland.

kir.pl

Chapter 2 –
THE EUROPEAN PERSPECTIVE

2.1 Services markets – local vs. international

The European market comprises 191 companies providing qualified trust services. All qualified services provided in one of the EU countries should be recognised in all other EU countries. In particular, electronic signatures and seals based on qualified certificates issued by qualified entities in other European Union countries must be recognised by public entities and consumer service providers. Such a competitive approach to the mandatory recognition of qualified certificates from other countries is expected to be a driver of services. Indeed, the data collected from trusted lists indicate that, in recent years, qualified trust services in Western European countries have shown tremendous growth.

Qualified trust service	Europe	Poland	Germany	Italy	Spain	France
Total number of service providers	191	6	10	35	26	22
Issue of certificates	167	6	8	35	23	14
Time-stamping	92	5	5	14	14	9
Preservation	1				1	1
Electronic registered delivery	11		2		3	4
Validation of signatures and seals	13	1			2	1

Comparison of qualified trust services in Europe, as at May 2019

Within the first two years of application of the eIDAS Regulation, services included on the lists were predominantly certificate issuance services. However, the last year saw the emergence of new services, such as preservation and validation of signatures/seals, as well as registered electronic delivery.

Trust service providers are subject to mandatory periodic eIDAS compliance audits and supervised by national supervisory bodies. While individual countries may not restrict the availability of foreign qualified trust services, they may impose additional obligations regarding national qualified trust services, or provide support, e.g. by providing access to national registries of identity documents. The extent to which law or supervising bodies restrict or support a qualified provider is indicated by the availability of the provider's services in foreign markets. The option to issue qualified certificates based on video verification, as described below, is a notable example.

The eIDAS Regulation permits issuance of qualified certificates upon verification of identity via non-direct means. Pursuant to these provisions, several qualified trust service providers have introduced a mechanism for issuing certificates based on video verification, allowing for qualified certificates to be issued without a face-to-face meeting with a certification authority representative. This approach not only simplifies the process of obtaining a qualified certificate, but actually enables services to be provided internationally.

Another solution, not yet available in Poland but offered by external qualified service providers, is the qualified one-time signature. A certificate for such a signature is issued for a single transaction or a group of transactions, does not require the user to memorise passwords or obtain additional admissions, and does not require a certificate revocation service. This approach makes it significantly easier to use qualified electronic signatures in business services for a single transaction, with the costs of issuing and using the certificate being covered by the service provider.

2.2 Notified identification schemes

An important aspect of the internationalisation of the services discussed in this report is enabling the interoperability of electronic identification means within European Union countries. Member States are required to recognise notified electronic identification means for online services, provided they meet the specified level of assurance (security). Notification means that a national means of identification is designated as accessible throughout the EU. Notification is carried out at the EU level and is preceded by pre-notification of the means by the Member State assuming responsibility for the security of the means. As at the date of this report, 17 notified and pre-notified electronic identification schemes have been published, covering various means of identification. The means most frequently notified are identity (ID) cards, some countries have notified mobile-based means of identification. Of note is the notification of identification means based around commercial service providers by Italy and the United Kingdom.

Poland has not as yet notified nor pre-notified any electronic identification means, but it is expected to notify the trusted profile at the substantial level and the personal profile (a new “e-dowód” ID card with an electronic layer) at the high level.

Availability of notified electronic identification means will also be of great importance with respect to trust services. Qualified registered delivery and issuance of qualified certificates for electronic signature may be performed on the basis of electronic identification means with the specified (substantial) security level, with notification serving as an actual confirmation of the quality of the identification means and its legal validation by the supervisory body of the country where the service is provided.

Country	Means of identification	Level	Status	Date
Portugal	Mobile key	High	PEER REVIEWED	10. 2018
Slovakia	Identification card Foreigner card		PRE-NOTIFIED	04. 2019
Portugal	Professional attributes certification system		PRE-NOTIFIED	05. 2018
Belgium	itsme® mobile app		PRE-NOTIFIED	04. 2019
Portugal	Identification card	High	NOTIFIED	02. 2019
Germany	Identification card Foreigner card	High	NOTIFIED	09.2017
Estonia	Identification cards Mobile tools	High	NOTIFIED	11. 2018
Italy	Identification card	High	PRE-NOTIFIED	11. 2018
Lithuania	Identification card		PRE-NOTIFIED	02.2019
The Netherlands	Identification means for businesses		PRE-NOTIFIED	12. 2018
Czech Republic	Identification card		PRE-NOTIFIED	12. 2018
Spain	Identification card	High	NOTIFIED	11. 2018
Croatia	Identification card	High	NOTIFIED	11. 2018
Belgium	Identification card Foreigner card	High	NOTIFIED	12. 2018
The United Kingdom	Electronic identification means managed by five companies and verified by GOV.UK	Low, Substantial	NOTIFIED	05. 2019
Luxembourg	Identification card	High	NOTIFIED	11. 2018
Italy	Electronic identification means managed by five private companies	Low, Substantial, High	NOTIFIED	09. 2018

Comparison of the notification status of electronic identification schemes in Europe, as at May 2019

2.3 The government administration in EU states and the EC regulator as a driver of services

Entities that carry out public tasks (the public services market) are obliged to recognise qualified and advanced signatures based on a qualified certificate. This obligation extends to all online services and applies to signatures based on a qualified certificate issued in any European Union country, provided that the signatures themselves were created in a reference format.

Many documents, even business documents, are created to serve as proof or evidence in administrative proceedings or court cases. Recognition of these documents by the public administration is the first step towards the full utilisation of electronic tools by businesses and individuals. That is why the eIDAS Regulation is focused on trust services which, by their nature, are commercially available solutions provided under market conditions, This is also the reason why Member States should not introduce their own tools and solutions that distort competition.

The common recognition of trust services at the European level is a great opportunity for growth, but it is also an immense technological problem, especially for public entities as far as recognition of qualified certificates is concerned. Trusted lists of all active qualified trust services, published by individual states, are a crucial measure in this regard. As mandated by the European Commission, lists of trust services are available from a single source – a list of lists. With these lists, it is possible to automatically verify whether a qualified certificate was issued by a qualified trust service provider.

The European Commission has also launched funding programmes to support solutions that enhance interoperability of electronic signatures. Libraries for verification of qualified electronic signatures and seals in any of the ETSI formats have been released as publicly accessible code.

2.4 Single European market

The eIDAS regulation is aimed towards achieving a single European market in the sense of mutual recognition of electronic signatures and seals based on qualified certificates issued in any country of the European Union. Mechanisms for verification of such qualified signatures are now widely available. However, local (domestic) providers who issue certificates after registering directly (via a meeting with a certification authority representative) are still very important. A growing number of certification authorities issue qualified certificates on the basis of remote identification (video identification).

In addition to services relating to electronic signatures and seals, the Regulation also makes reference to electronic registered delivery services. These services, despite their obvious convenience in interactions between administration, companies and natural persons, have been only developed independently in individual EU countries and have not been widely adopted. The qualified registered electronic delivery services currently available are provided by operators limited to 5 countries, and are used exclusively for delivery of documents on a domestic level. Delivery services have been slow to take off because public entities are not required to accept deliveries made through this method, and because the technical standards governing the functioning of these services were adopted by the standardization committee as late as at the end of 2018 and the beginning of 2019. Establishing uniform rules of acceptance of qualified electronic delivery mainly – especially by public entities and providers of consumer services – will serve as the driver for growth of these services throughout the EU.

The table below shows a comparison of various electronic signature solutions. Among the presented features, recognition is of particular importance, as it is synonymous with establishing a single European market

Feature	Qualified electronic signature	Personal electronic signature	Trusted electronic signature
Assurance	Qualified signature	Advanced signature	Simple signature
Awareness	Pan-European	Poland	Poland
Verifiability	Automatic e.g. Adobe or validation services	Manual – needs to be configured	Manual – needs to be configured
Applicability	Administration Business	Administration Optionally business	Administration
Signatory	Citizen Official	Citizen	Citizen
Remote signature	Optional	No – card only	Yes
Electronic form equivalent to hand-written form	YES	NO	NO
Registration	Face-to-face/remote	Face-to-face	Face-to-face/remote

2.5 Changes in standards and certification

Technical standards now exist for each area of trust services. The issue of certificates, creation of signatures, creation of time stamps, and other trust services have been well-defined by technical standards. Standards governing remote signatures and registered electronic delivery were developed and published last year.

Services	Standards
For service providers	ETSI EN 319 401 General policy requirements for trust service providers
Issue of certificates	ETSI EN 319 411-1 Part 1: General Policy and security requirements for TSPs issuing public key certificates ETSI EN 319 411-2 Part 2: EU qualified certificates
Creation of signatures	ETSI TR 119 100 Guidance on the use of standards for signatures creation and validation ETSI TS 119 101 Policy and security requirements for applications for signature creation and signature validation ETSI TS 119 102 Procedures for Creation and Validation of AdES • Part 1: Signature creation and validation • Part 2: Signature Validation Report
Remote signatures	ETSI TS 119 431-1 Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD ETSI TS 119 431-2 Policy and Security Requirements for TSP Service Components Supporting AdES Digital Signature Creation ETSI TS 119 432 Protocols for Remote Digital Signature Creation
Time-stamping	ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles
Preservation	ETSI TS 119 511 Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (draft) ETSI TS 119 512 Protocols for trust service providers providing long-term data preservation services (draft)
Electronic registered delivery	ETSI EN 319 522 Electronic Registered Delivery Services (ERDS) ETSI EN 319 532 Registered Electronic Mail (REM) Services ETSI EN 319 521 Policy and Security Requirements for Electronic Registered Delivery Service Providers ETSI EN 319 531 Policy and Security Requirements for Registered Electronic Mail Service Provider
Validation of signatures and seals	ETSI TS 119 441 Policy requirements for TSP providing signature validation services ETSI TS 119 442 Protocol profiles for trust service providers providing AdES digital signature validation services
Trusted lists	ETSI TS 119 612: Trusted lists

REPORT EXPERT

Michał Tabor
Partner / Board Member, Obserwatorium.biz

Over the past 3 years, the EU trust services market has expanded to include over 190 companies providing qualified trust services, recognised by public institutions and courts of all Member States. Most of these services are centred around issuing qualified certificates for electronic signatures and seals. I predict that, as the market grows, two parallel developments will occur. First, additional qualified services – beyond certificate issuance – will become available. In particular, development of electronic delivery and validation services for electronic signatures are areas that I see as extremely promising. Secondly, trust service providers operating in multiple markets at the same time and offering a wide range of trust services will play an increasingly prominent role. This will result in increased competition on local markets, which have so far been divided between domestic trust service providers, and this competition will force a better product range and easier access to services.

REPORT EXPERT

prof. dr hab. (Prof. Ph.D.) Dariusz Szostek
Partner, Szostek & Bar Law Firm

Throughout the late 2010s, cloud-based and paperless solutions have been growing in popularity in developed counties, both within the digital economy and within sectors that utilise new technologies. Operators have not only adopted e-workflows, but have also largely moved away from traditional paper workflows in business processes and replaced them with fully digital information workflows. Countries (such as Estonia, Dubai, etc.) have increasingly eschewed traditional data/information workflows (and thus also paper workflows) in favour of fully digital workflows, and have been increasingly adopting technological solutions based on tokens, smart contracts, DLT and blockchain. The so-called digital revolution 3.0 is based completely upon digital information workflows and digital records. Another important development in the European Union are the EU regulations directly or indirectly supporting – or even mandating, in some cases – electronic workflows. GDPR is but one example of that – with the volume of contracts and agreements, the cost of traditional document processing, disclosure obligations, and the right to be forgotten, the regulation actually promotes and compels the use of paperless procedures. Legal regulations of the Digital Europe 2020 project fully provide for such activities.

SIGNICAT

Trusted Digital Identity

Signicat provides **Digital Identity Verification**, **Authentication**, and **Signing solutions** for regulated industries.

- **Identity Verification**
- **Advanced Authentication**
- **Electronic Signing and Archiving**
- **Cross Border Digital Identity**
- **Digital Identity Service Provider**
- **Identity Assurance as a Service**

www.signicat.com

Chapter 3 –

COMMERCIALISATION POTENTIAL OF eID AND TRUST SERVICES

3.1 Introduction

Electronic identification and trust services have an advantage over other tools used in the development of on-line business processes – they all fall under unambiguous legal interpretation and must meet standardised security requirements.

The chapter on the current situation on the electronic identification market and trust services already presented a basic overview of current applications of such services – for example, the use of qualified electronic signatures in dealings with the public administration. This part of the report will focus primarily on those business processes where eID and trust services are not currently used or are used on a limited basis. The clear advantages of eID and trust services – resulting from their standardisation, precise legal framework, the validity stemming from their legal status as proof/evidence, and the restrictive process of certifying qualified entities – all support the case for eID and trust services being implemented as an alternative to current digital solutions, or perhaps even serve as a strong argument for strategic migration of selected processes to electronic channels (or designing them, from scratch, with full end-to-end digitalisation in mind).

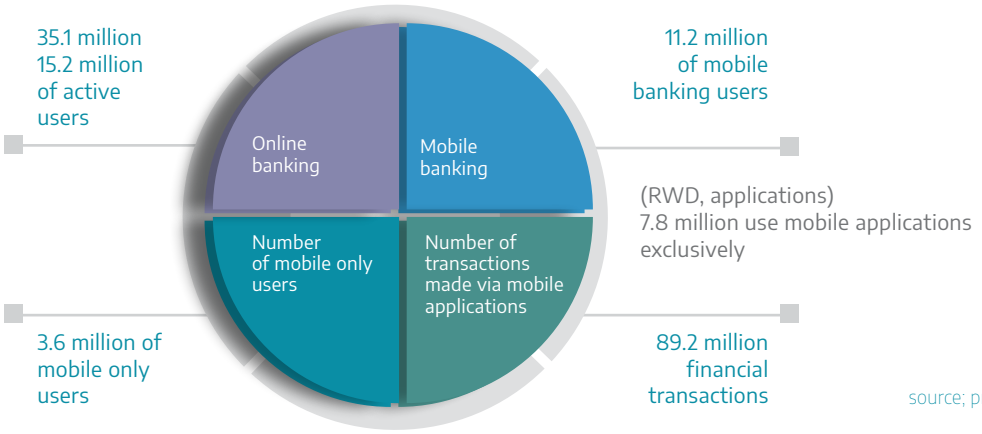
3.2 eID as a basis for successful commercialisation of digital services

Proliferation of electronic identification services is key to the success of trust services in Poland.

Just as in previous publications (the dedicated reports published in 2017, namely "eID Report – Electronic Identification in Poland" and "Breakthrough in On-line Services – Development of Trust Services in Poland"), we argue that commercialisation of business services built around trust services cannot succeed without mass take-up of electronic identification (eID). We again point to the potential of the banking sector, which has the largest number of active users of digital channels (over 15 million active users of online banking). Those users first underwent secure identification in accordance with legal requirements – most often though branch-based channels. Maintaining regular contact with the bank also prompts the need for proper digital hygiene, i.e. proper management of access to passwords and applications by the users. This makes them a viable tool for accessing government e-services, such as the Polish Identification Schema for eGOV ("Profil Zaufany") or mTożsamość (the latter of which is accessible via the

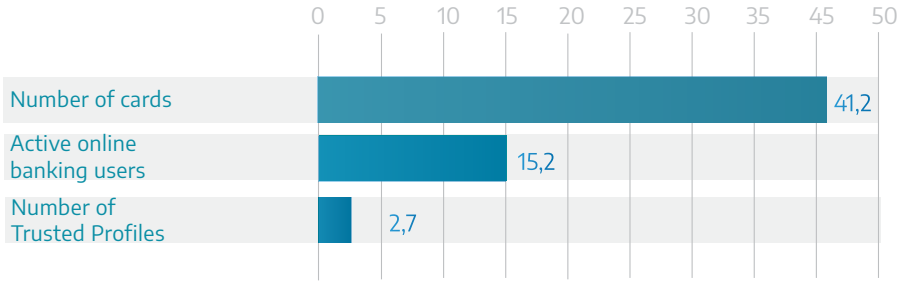
mobile ID application (mObywatel)). Also worth noting is the potential of payment cards, whose ubiquity and extensive acceptance infrastructure seem to make them a candidate for a target medium of electronic identification (one that would also be based on banks).

Number of users of electronic banking channels – individual customers



source; prnews.pl, Bankier.pl

Numerical comparison of Trusted Profiles, payment cards and active online banking users (in millions, 2018)



As mentioned in the previous chapter, the identity card with an electronic layer (e-dowód) is in an early stage of implementation, and the migration process is expected to take up to 10 years. For these reasons, it is difficult to determine how useful this tool is for commercial processes at this stage of its development.

3.3 Commercialisation potential – the "hygienic" prerequisites

From a business standpoint, eID and trust services should be some sort of a "toolbox", one that can be used by managers or decision-makers attempting to develop new business processes or modify current ones – to optimize or digitise them, for example.

We believe that the following "hygienic" conditions, essential for the wide adoption of electronic identification (eID) and trust services, are currently in place in Poland:

Currently, companies are aware of the various types of tools for remote identification of customers or trust services (with the notable and sole example of the qualified electronic signature, which is generally and stereotypically considered to be a non-ergonomic and expensive tool). However, these companies are striving to develop the processes on their own. It is therefore important to foster awareness among managers responsible for the digital transformation of their companies or sales and electronic transactions (e-commerce), so that they know how to incorporate trust services into modified or new processes and achieve end-to-end digitalisation.

AN IDEA

- an integrator of eID and trust services, operating like a payment integrator

Currently, electronic payments are implemented when a new online store is created – without e-payments, it is impossible for a company to thrive on the market. To avoid developing a proprietary solution, which is not desirable from a financial standpoint, the system is instead integrated with one of the payment integrators available on the market. If we manage to 'secure' similar integrators for eID and trust services on our market, with which service providers will be able to connect in an almost "plug & play" manner, this will mean a wide take-up and commercial success of these services

2. eID/trust services availability and ease-of-use

Availability, in this case, is understood as ubiquity of the tools necessary for implementation of eID processes and trust services. As indicated above, we believe that building trust services around electronic identification is key to popularizing them. Such electronic identification may in turn be based on widely available tools, such as access to ID cards (with or without an electronic layer), banking electronic channels, payment cards or even the Trusted Profile.

AN IDEA - electronic identification and trust services should be just as easy to use as pay-by-link online transfers ("what >>everyone<< does").

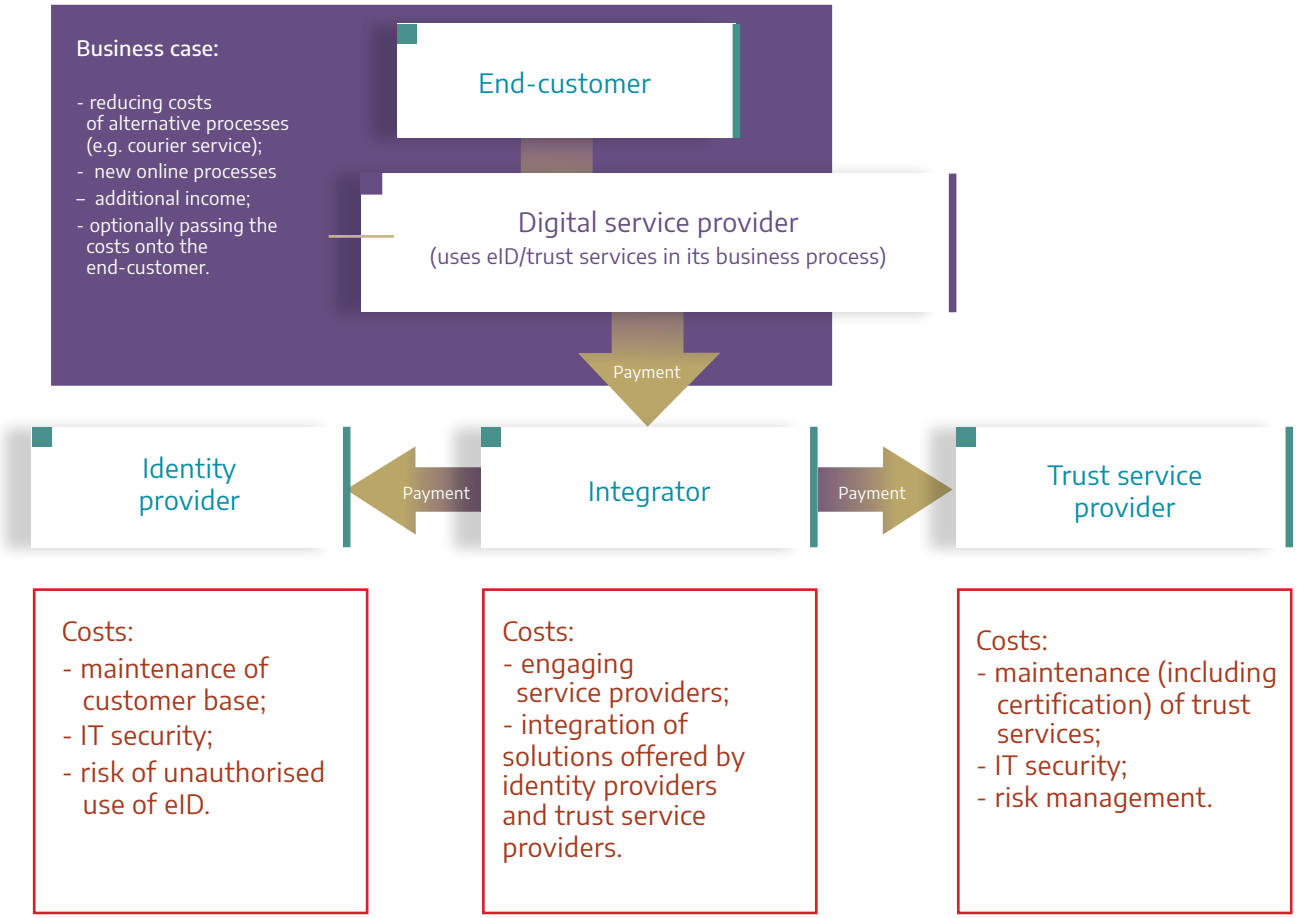
3. Support from the regulatory environment and its stability

The EU regulations on eID and trust services, based around the eIDAS Regulation, are formulated to ensure legal certainty and apply throughout the Union. At this initial stage, the joint requirements for state institutions concern the acceptance of qualified signatures and electronic seals. The inclusion of trust services in the requirement to notify other countries of domestic legal provisions provides stronger control over local solutions that could distort competition within the market. Nevertheless, Poland does continue to pursue policies aimed at limiting competition within the market and introducing domestic solutions – for example, granting privileged status to the personal signature on a national level.

4. Attractive business model for using eID and trust services

Developing an appropriate business model attractive to all parties in the transaction chain – i.e. eID and trust services – is a key prerequisite to successful commercialisation of this market. Failure to develop a model and understand the expectations of individual players may result in years of halted growth for the market, despite the legal and technological readiness and the potentially positive response of customers who want such solutions.

Target business model for eID and trust services



The business model of eID and trust services outlined above uses a similar scheme to that used for payments, wherein the service provider pays eID and trust providers a fee (via a business-technology integrator or, in some cases, directly) for using these services in its business processes, then offers the same services to its end customers (consumers or businesses). For the purposes of the following analyses, we assumed a value of a single "transaction" of PLN 10 (about 2 EURO) as the sum of fee paid to the integrator by service providers with reference to processes involving eID and trust services (e.g. using a qualified signature "on the fly" based on bank-provided electronic identification), in the case of eDelivery the amount was set at PLN 1. In both cases, the amount is a function of potential reference market values, i.e. necessary alternative costs – ROD when using a courier service which confirms the client's identity, or sending a registered mail with acknowledgement of receipt through the post.

CASE STUDY

Santander Bank Polska: taking the plunge into trust services

Santander Bank Polska (formerly Bank Zachodni WBK until 7 September 2018) is the third largest bank in Poland in terms of assets and one of the market's most successful adopters of modern technologies, which play an important role in formulating the bank's market strategy. In 2017, the bank decided to implement the qualified electronic signature and other cloud-based trust services in its internal banking systems. A partnership with Asseco Data Systems resulted in the bank implementing the Platforma Usług Zaufania Online ("Online Trust Services Platform"). Thus, Santander Bank Polska became the first bank in Poland and one of the first in Europe to give its employees the option to digitally sign and transfer the bank's internal documents.

The Platforma Usług Zaufania Online is an internal portal that enables bank employees to use the electronic identification tools provided for in the European eIDAS Regulation. By adopting this solution, the bank was able to implement the electronic seal and the qualified electronic signature in its internal processes, as well as the SimplySign mobile signature created through a mobile application for smartphones and tablets.

The result was improved management of the bank's internal workflow and eliminating the need for signing documents by hand. The bank's internal processes were greatly streamlined, and signed documentation could be immediately delivered to the recipient. The change also led to reduced costs and reduced the time needed to complete business processes.

Furthermore, the platform allowed the bank to fulfil the requirement to implement a so-called "durable medium". This enabled electronic delivery of requisite communications to customers on new fees, changes in terms and conditions, etc.

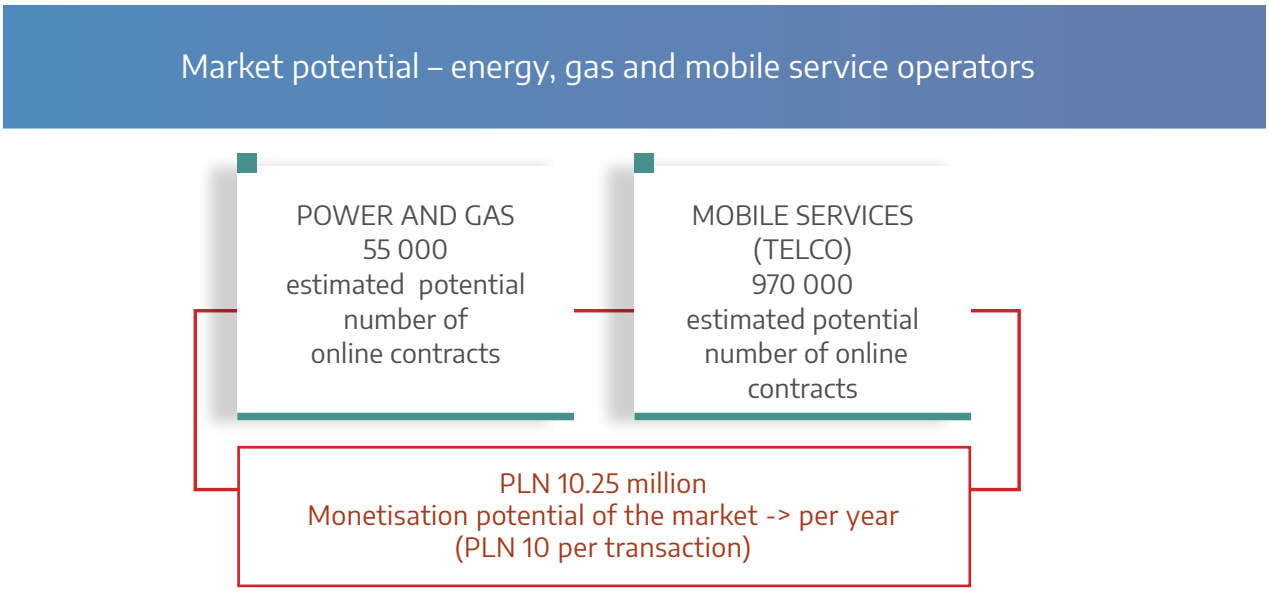
The platform conforms to rigorous banking procedures. It has been adapted to the bank's internal systems and connected to an external Authorisation Centre, which acts as a so-called 'trusted third party'. The qualified mobile electronic signature and remote electronic seal work via cloud technology. The functional scope of the solution includes leasing and factoring services, as well as external dealings – contracts with providers, communication with customers and brokerage houses, eKRS financial statements, etc.

We are proud to have been trusted by this bank and we hope that it will open up venues of co-operation in other areas that Asseco Data Systems specializes in. The Platforma Usług Zaufania is the first cloud-based solution of its kind in Poland. This project has shown that SimplySign, the qualified mobile signature created by Asseco, is not only a product for entrepreneurs or accountants who sign documents electronically, but also a new technological tool of unlimited application, simplifying communication between enterprises, the government and citizens – says Artur Miękina, Key Projects Sales Director, Security and Trust Services Unit, Asseco Data Systems.

3.4 Commercialisation potential – selected business areas

3.4.1 Concluding contracts / making statements of will

A flagship example of further application of eID for handling signatures and transactions remotely are the various service contracts, especially contracts for services/utilities for homes and small businesses, where one party is a consumer or entrepreneur (usually self-employed), while the other is a provider of such services – electricity, gas, internet, home phone services, or mobile operators (though there are other potential applications, like contracting property protection or property insurance services).



It is estimated that the number of instances of individual customers and companies (sole proprietorships, SMEs) switching their electricity and gas supplier in Poland is 184 thousand a year. Assuming a digitalisation ratio of 30%, we can suppose that the number of such operations that could be potentially performed remotely, i.e. with electronic identification and signature – without visiting the branch office of the supplier or its agent – is 55 thousand per year. In the case of contracts for telecommunications services, an estimated 3.105 mln individual and corporate customers (sole proprietorships, SMEs) change their operator per year (excluding renewal of services at the same operator, which can often be done remotely via telephone or even via the provider's mobile or online electronic customer service, so the commercial potential of applying eID and trust services in this particular context should be considered limited). Assuming again a 30% ratio yields a potential 970 thousand mobile telecommunication service contracts that can be concluded by customers through the use of eID tools and the trust services built around them (specifically electronic signature).

If we apply the "transaction monetisation rate", as defined above, the resultant revenue potential totals PLN 10.25 million per year.

The legal framework is based around the existing regulations concerning electronic identification – eIDAS and the Act on trust services ("ustawa o usługach zaufania"), as well as the "domain" acts, i.e. telecommunication law and energy law. One important amendment that affected telecommunications sector was introduced in December 2018, enabling the use of the so-called document form ("forma dokumentowa") and the effective conclusion of contracts using means of identification created by banks.

Using eID to sign contracts in traditional channels is another promising application. Electronic identification that utilises a payment card issued by a Polish bank, or the new ID card with an electronic layer (the "e-dowód") may be successfully used for this particular purpose. Such a process may reduce the use of fake IDs and facilitate the "de-papering" of contracts, for example by using a biometric signature created on a tablet at the point of sale, or by using SMS authorisation.

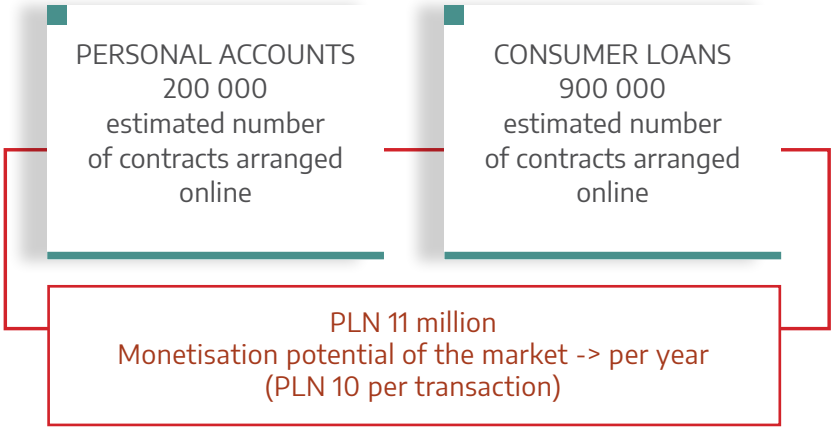
REPORT EXPERT

Dagmara Malinowska
Rachuneo.pl

There are still industries in Poland that have successfully resisted digitalisation or do not consider it to be an opportunity for business growth and reduction of operating costs. When designing Rachuneo's utility price comparison website, we conducted several dozen interviews and surveys, which clearly show that customers are looking for the same conveniences they get from other industries. If they can buy insurance, book a trip, or open an bank account online, why shouldn't they be able to conclude power, gas, TV or internet service contracts through the same channels? What is telling is that this reluctance is mostly limited to large state-owned entities, with the honourable exception of PGE, whose subsidiary Lumi PGE has just offered customers the option to sign documents electronically. Private suppliers are more inclined to offer their customers the convenience of signing contracts online. It also reduces selling costs and costs of handling contracts. Digitalisation in this area is therefore a solution beneficial to all parties.

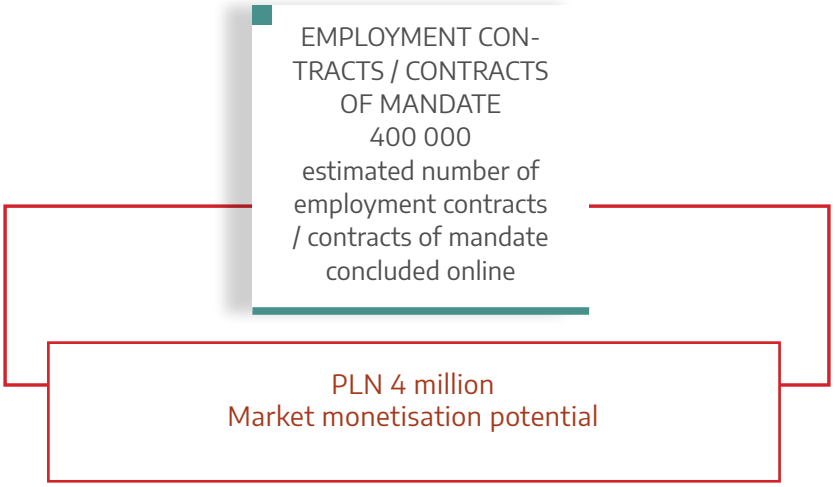
At Rachuneo, it is our ambition that all contracts with utility companies – energy and gas suppliers, telecommunication service providers – be concluded digitally on our platform. To that end, we would welcome a chance to work with all utility companies and facilitators of digital processes – such as eID and trust service providers.

Market potential – financial services



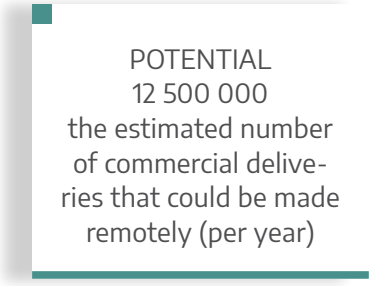
The financial services market was one of the first to undergo digital transformation. 95% of repeatable operations, such as deposits, withdrawals and transfers, are already conducted over remote channels such as ATMs or online/mobile banking systems, outside bank premises. The sale of products, such as deposit or credit products, and the subsequent conclusion of contracts between the bank and the consumer also takes place via electronic channels. The traditional channel is still commonly used for 'onboarding', i.e. the process of bringing in a new customer, which usually entails setting up a personal account and a package of additional services (payment services, access to electronic channels, etc.). We estimate that around 200 thousand personal accounts are currently set up in a remote formula – primarily with the use of tools such as "authorised transfers", video verification, or the traditional signing of contracts in the presence of the courier delivering the documentation. Therefore, this is where the more secure and standardised eID services and electronic signatures should be used – provided that the ease-of-use of current solutions is preserved in the process. The second area, which is much larger quantity-wise, is cash loans. They have been growing more and more popular throughout the last decade and represent an increasingly notable alternative to banks, which were somewhat late in implementing solutions enabling the provision of easy "one-click" cash loans or credit cards. We estimate that up to 900 thousand contracts are concluded annually via electronic channels (websites, mobile applications). If we assume the monetisation ratio specified above, this segment of the electronic identification and trust services market may be worth as much as PLN 11 million in total. Other business areas where this mechanism could be applied include onboarding processes of companies (e.g. setting up current accounts) and onboarding processes of investment funds and similar entities (first-time acquisition of units in the fund, including the MIFID questionnaire), insurance companies (e.g. purchasing life insurance) or FX trading platforms.

3.4.2 Concluding employment contracts



Another area where eID and trust services may prove useful is the conclusion of employment contracts and contracts of mandate. The amendments introduced in January 2019 have resulted in a less restricted environment in terms of employee records digitisation. We estimate that about 400,000 contracts of this type are concluded remotely, which would mean that the potential for monetisation of this particular segment of the the eID and trust services market can be valued at around PLN 4 million.

3.4.3 Electronic delivery (e-delivery)



The development of a public electronic delivery process, announced by the Ministry of Digitisation and other entities, may potentially open up the market for commercial e-delivery solutions, mainly for the B2B segment – after all, confirmation of receipt is important for business correspondence due to the consequences stipulated in specific contracts between business entities. The implementation of qualified services , i.e. “an electronic registered letter with confirmation of sending and receipt”, would streamline and accelerate a number of economic processes. This solution could be provided by commercial qualified trust service providers under existing regulations on electronic identification and trust services – eIDAS and the Act on electronic delivery. Appropriate amendments could also be made to the Polish Code of Administrative Procedure, if a comprehensive analysis of individual business segments indicates that such changes are necessary.

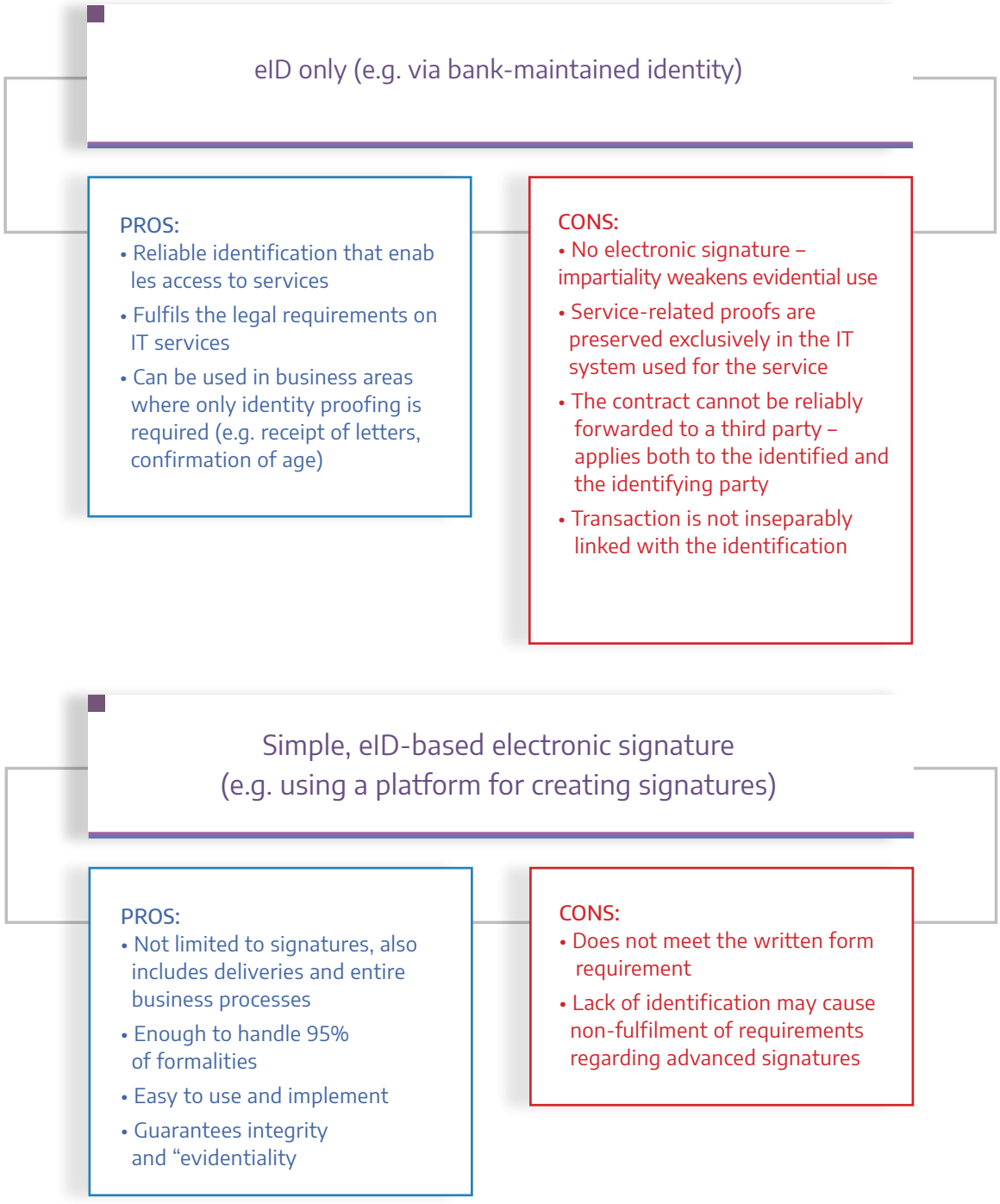
3.4.4 Variant of eID use – confirmation of selected data

eID tools can also be useful in processes where legal regulations – or, indeed, the business nature of the service – require that a trusted third party verify certain attributes of the customer. One of such potential uses is for confirming age of majority – an available eID tool, used either on-line or in the physical would, may help verify age of persons buying alcohol, visiting a bookmaker's outlet or attending clubs, if the provider wishes to bar minors from accessing the service. Also, eID may become an attractive means of optimising selected e-commerce processes or collection of parcels (e.g. from the "Paczkomat" parcel lockers) by providing additional confirmation that a parcel has been collected by an authorised person (the process referred to as "personal electronic delivery"). The increasingly important issue of customer data protection (GDPR) and the related fact that customers are becoming increasingly aware of their rights, may also successfully foster the use of eID services. After all, a service provider – for example, a ski rental – may feasibly verify a customer's identity by using a payment card, an identity card, the "e-dowód" or a similar tool without ever needing to process any data themselves and engage in objectionable practices by making photocopies of ID documents. Employee Capital Plans are another example, wherein the process of onboarding/registering decision-makers in participant companies in individual institutions that coordinate the plans, and with regard to end-customers (employees), may be developed to take advantage of the effectiveness and legal security provided by eID and trust services.

3.4.5 Choice of eID tools and trust services for individual commercial processes

The next section presents the strengths (pros) and weaknesses (cons) of using various configurations of electronic identification (eID) and trust services. This comparison was made with the assumption that the specific tools are used for the purposes of a business transaction which gives rise to a commitment of the identified party or which reaffirms an action of theirs.

PROSPECTIVE SCENARIOUS OF eID AND TRUST SERVICE APPLICATION



Qualified, eID-based electronic signature (e.g. “on the fly”)

PROS:
- Equivalent to the written form
- Recognised universally throughout the EU
- Unequivocal evidence in court proceedings
- Easy to implement for identification users
- Available via browsers, online systems and mobile apps
- Transaction-based risk.
- One-time charges for on-the-fly signatures – no time-limited purchase of signature required

CONS:
- The solution is bound to the service provider, regardless of the customer
- Fee charged at each transaction (by the customer of digital service provider)
- Identification required for each individual transaction.
- Fees for issuing qualified certificates
- No functional solutions from Polish providers
- Each certification request has to be accepted separately (at each instance of signature creation)

Limited to simple electronic signatures (e.g. using a platform for creating signatures)

PROS:
- Enough to handle 95% of formalities
- Easy to use and implement
- Guarantees integrity and “evidentiality”
- Identifies the signatory and ensures that the transaction is linked to them

CONS:
- Not equivalent to the written form
- In evidential proceedings the burden of proving the validity of the signature lies with the applicant

REPORT EXPERT

Marcin Szulga
Department Director
Security and Trust Services Division
Trust Services Research and Development Department

What are the directions for technological development at Asseco Data Systems?

Maintaining the leading position on the Polish trust services market and expansion on the European market require us to implement technologically advanced development plans. We are focusing on the move towards the large business segment. Large businesses expect services that are readily accessible and stable, as well as efficient and scalable to an extent unattainable on the retail and SME markets. This challenge can be met by combining our analytical expertise with the use of new technologies. That's how we've been able to conduct 3 million SimplySign mobile signature transactions a day.

Our market expansion strategy also involves solving our clients' business problems by extending the functionality of our products. We are introducing new methods of onboarding with tablets and biometric signatures for qualified certificates. We are working on video identification and registration methods that utilise reliable identity databases from financial services providers, so that clients can register without ever appearing personally at the registration point. This will enable us to further expand into foreign markets.

We are also introducing the „on-the-fly" signature service for settling one-time transactions.

We are developing tools to support scaling of paperless processes. To that end, we are focusing on expanding a next generation signature app, in particular the Signer system, which integrates all of Certum trust services and packing them into an intuitive, integrated interface.

REPORT EXPERT

Tomasz Sekutowicz
SignHero

We have conducted hundreds of interviews with entrepreneurs, and those observations still lead me to believe that the mentality comes first, with education second.

Why mentality? Often due to historical reasons, but also because of a certain fear of the new. Polish entrepreneurs, especially SMEs, are as a group particularly exposed to constant legal changes, while at the same time kept busy by everyday life and lack of time. The everyday reality of the issue of a paper letter signed by hand is still a model for interactions between entrepreneurs. The officials supervising them are exactly the same, the first thing they ask for is ... "file binders with the documents". How to overcome these stereotypes and this mentality? In my opinion, sound education is the only way. In fact, the wide digital services market, the paperless segment should unite to properly educate the market. Then, by instructing both the entrepreneurs from various industries and the consumers, we will create a bottom-up need for digitalisation, overcoming the fear of the new and of the ever-omnipotent controller asking for the binders. Consumers or entrepreneurs who know that they can sign a contract with a contractor using a platform for signing, a qualified certificate, or an ordinary e-mail will operate more efficiently in a very competitive economy. They will be equipped with the knowledge that the officials and the courts are obliged to admit specific electronic proofs and evidence. The attitude towards digitalisation is changing – there are industries, new businesses, and startups which focus on digitalisation and „paperless" processes from the very start, as something that's in their "business DNA". Even now, this trend is quite pronounced in corporations, power companies, and telecommunication operators.

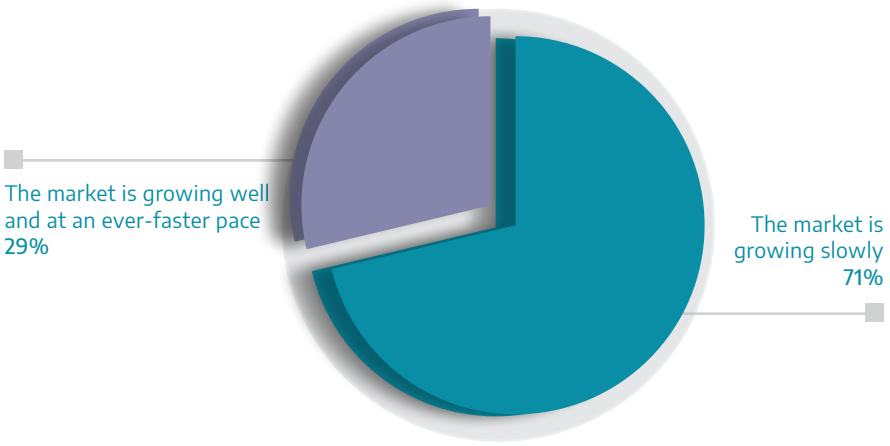
Integration of the signature platform SignHero with the learning service Lingroom. It serves as an interesting example of communities coming together, of overcoming mental barriers and of the aforementioned education efforts. Thanks to the initiative, students can benefit from modern, digital, remote language learning. The teacher can leave the shadow economy behind and earn money legally by signing a contract without ever printing a page, all in accordance with the latest letter of the law regarding unregistered business activity.

3.5 Commercialisation of eID and trust services – survey results

As part of research for the report we secured the participation of eID, trust and digital service providers, who gave us an assessment of the current state of the market and made some predictions for the next 12 months.

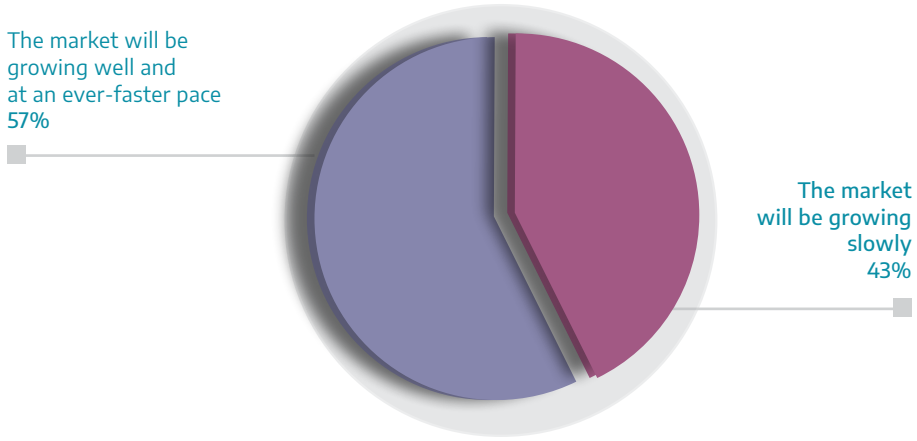
All of the respondents have positively assessed the development of the eID and trust services market, while noting that its growth is slow.

Assessment of the current state of the eID and trust services market



The respondents see the potential for the market to grow quickly within the coming 12 months.

Assessment of the growth of the market within the coming 12 months



Representatives of service providers have also stated their opinion on the commercialisation potential of eID and trust services for the selected sectors, in particular for the energy, telecommunications, medial services, IT, public administration and financial sectors.

The financial sector is definitely perceived as the most promising in terms of commercialisation, which can be attributed to the well-regarded solutions that have been implemented by the sector, its openness towards the new, and the business potential in terms of eID and trust services.

Commercialisation potential in the financial sector:	
Mean (1-10):	8.71
Mode:	10

High potential

Reasoning:
High awareness, wide B2C network, successful deployment of solutions thus far

The potential in the telecommunications sector is also rated highly – respondents pointed out that the adopting eID and trust services would improve competitiveness, they also mentioned the need to sign multiple documents and the shift towards remote customer onboarding.

Commercialisation potential in the telecommunications sector:	
Mean (1-10):	7.71
Mode:	9

High potential

Reasoning:
Good area for implementation due to the "remote nature" of the sales process, SIM registration system

Commercialisation potential in the medical services sector:	
Mean (1-10):	7.07
Mode:	5

Fairly high potential

Reasoning
Frequent business-to-client contacts and a large volume of documents to sign on the one hand, on the other – legislative problems and low pressure from the customers to "digitise" medical services, the presence of competitive public services.

The medical services sector also placed high on the ranking. The respondents noted the need to process (and sign) a large number of documents in medical processes. On the other hand, there is the issue of sensitive data, potentially detrimental to commercialisation as it may cause customers to adopt low expectations regarding digitalisation of medical services.

Next was the public administration sector. Its lower ranking may be largely a result of the free tools that are already being provided as part of public solutions (e.g. trusted signatures, personal signatures) and may be used in everyday dealings with the public administration.

Commercialisation potential in the public administration:	
Mean (1-10):	6.71
Mode:	9

Fairly high potential

Reasoning:
On the one hand, the government produces its own solutions, on the other – it is in a good position to popularise them. Most tools are free-of-charge

The IT services sector is regarded as having fairly high potential due to the growing interest in the security segment, which is undoubtedly convergent with trust services.

Commercialisation potential in the IT services sector:	
Mean (1-10):	6.71
Mode:	9

Fairly high potential

Reasoning:
Growing interest and security focus, but B2C interactions are infrequent and the market is saturated

Commercialisation potential in the field of human resources:	
Mean (1-10):	6.29
Mode:	7

Potential limited, but above-average

Reasoning:
Contracts may offer opportunities for commercialisation, but the demand is low

The potential for commercialisation in the field of human resources, the real property sector and the energy sector were rated as limited to low. The respondents mainly indicated the following reasons behind the low commercialisation scores:

- Low demand for trust services from end-users (e.g. the recruitment segment)
- Lack of awareness of electronic identification and trust services among service recipients (real property segment)
- Low competition on the market, customers rarely switch providers – energy sector

Commercialisation potential in the real property sector:	
Mean (1-10):	5.86
Mode:	3

Low commercialisation potential

Reasoning:
Lack of awareness, the potential is there, but perception of eID and trust services must first change. Risk.

Commercialisation potential in the energy sector:	
Mean (1-10):	5.71
Mode:	9

Low commercialisation potential

Reasoning:
State control of the sector, customers tend not to switch providers, low competition

REPORT EXPERT

Tomasz Chomicki
President of the Committee on Digital Administration
Polish Chamber of Information Technology and Telecommunications

The last few years have seen a rapid growth of trust services worldwide. Recently, we celebrated the twentieth anniversary of the electronic signature in Poland, which was a new glimpse into the modern world. The times are changing, and those changes present ever-new digital challenges for technology companies. They are creating new services and solutions, with emphasis put on mobility, data security, and on the speed and flexibility of the new solutions. Cyber security has become essential to the operation of the "Digital Identity" market. It is important to remember that solutions dealing with sensitive data as a key component were subject to standards-based certification – the Common Criteria.

We welcome the fact that Poland has seen the release of publications such as "Commercialisation of eID and Trust Services in Poland and Europe", a report prepared by a group of exceptional experts in the field of trust services.

Chapter 4 –
MARKET DEVELOPMENT SCENARIOS

4.1 Introduction

The previous chapters described a variety of solutions and services designed to provide security measures for online services and to enable conclusion of distance contracts. They examined the potential of commercialisation within individual business areas, as well as the main market trends, as indicated by the cited experts. Considering the legal regulations and the maturity of the services offered, it is reasonable to argue that both the user awareness among users and the take-up of these services will grow with time. We would now like to present the scenarios for the development of this market with regard to the evolution of:

- tools;
- service recipients (consumers) and service providers (businesses);
- business growth.

4.2 Development of tools

Trust services based on eID will play a significant role

Yes – eID services are needed to register for trust services, they are the first step in the process of issuing a certificate, and a compulsory component of electronic delivery. Electronic identification is a unified and legally recognised method of identity proofing, and therefore also required for qualified services. We already have electronic identification means whose assurance levels have been validated by the Minister of Digitisation by deeming them acceptable for trusted profile creation – it is only a matter of time before they are also used for qualified services.

Tools of electronic identification – identity card, video verification

For trust services to function, there need to be electronic identification services available, ones which draw upon the primary source of state registers and identity documents issued on the basis of those registers. The new electronic ID card will eventually help automate registration for trust services, but it will take several years before this new e-card finds its way into the wallets of all citizens. For now, the fastest method of identity proofing widely available in other countries is video verification, which can be used, in particular, to issue a qualified certificate

without the need to visit an identity verification point. Solutions built around video verification will be the primary means of verification in the coming years, supported by other techniques as necessary to ensure security, whereas the electronic ID card has the potential to ultimately become the main method of verifying the identity of citizens within these pivotal electronic processes.

Biometrics are still a controversial topic, though they have found widespread use in mobile phones (for unlocking the phone with a fingerprint scan and face recognition) and payment transactions. All methods of biometrics that will support user authentication without significantly affecting usability will be useful for trust services and will serve as the main or supporting component of security systems, depending on the security level of the given method. Behavioural biometrics will play an increasingly large role in regard to the latter function, providing additional information based on an analysis of user behaviour to assess the risk related to transactions made using electronic identification or electronic signatures.

Media and tools for trust services

When the first qualified certificates were entering use over a decade ago, all providers on the market used cards as the basis for their solutions. The main ease-of-use improvements made over the years were the reduction of the size of the card and providing it in the form of a USB key. The disadvantage of the card is that it requires drivers to be installed on the system used with the card. Qualified signature solutions for remote creation of qualified signatures are now available in Poland, following the general trend towards virtualisation of solutions. Such solutions are becoming more and more common and will eventually replace the card in consumer applications, whereas the card itself will be used for situations where natural persons create multiple signatures every day, in a well-defined environment.

The new electronic ID card – is it going to change the market?

The new ID card with an electronic layer (the so-called “e-dowód”), deployed in March 2019, introduced 4 main electronic functionalities: transmission of the holder’s verified data, confirmation of attendance, electronic identification and personal signatures. All of these components will be increasingly applied as security measures for citizens’ interactions with the authorities, banks and companies, both face-to-face and digitally. In the first phase, the ID card will be used mostly for securing current ID verification functions via the electronic layer, e.g. when applying for loans. The ID card should play a huge role in identification of citizens

in public services, or in trust and financial services. On the other hand, due to its importance in the private affairs of each citizen, the card should not be used as a tool for creating signatures and confirmations on behalf of companies and authorities, as it could then become an excellent potential tool for compromising the security of the card holder.

Durable medium and electronic delivery

The institution of a durable medium was established in response to the lack of registered electronic deliveries. The durable medium should be replaced with solutions which will not only guarantee the integrity of the data, but also provide confirmations that the data has been sent to and received by the consumer.

The main obstacle to the development of electronic delivery services in Poland is the lack of legal mechanisms permitting government administration to accept documents through this channel. Restricting the exchange of documents to the in-house systems of individual offices and the ePUAP portal will fail to promote growth of electronic services in Poland. Electronic deliveries are gaining more and more acceptance in the European Union states, and they should also be expected to grow in Poland in the near future. The proposed Act on electronic delivery, depending on its final provisions, may either lay down foundations for parallel functioning and recognition of qualified registered electronic delivery services by public administration or, by introducing a single model of subsidised public electronic delivery service, repeat the errors of ePUAP. At the moment, electronic delivery services in Poland are few and far between, limited to those provided by Envelo, Bankmail and Autenti. None of them are qualified services, and each follows the company's own internal standards. The situation is similar in the EU member states, where the number of qualified RED services is limited to 11, but it should be noted that the standards governing the provision of such services were published only within the last six months.

Electronic seals

Using electronic seals for all online services significantly streamlines both administrative and corporate processes. Great improvements in efficiency could be made by introducing provisions that would permit government agencies to issue decisions and other documents sealed with the qualified seal of the agency (rather than signed by it). The seal will not replace signatures for the purposes of making declarations of will, but it would be the best solution in cases where documents need to be issued automatically with proof of origin. The electronic seal will become the basic attribute of an official document, at least for those applications, as long as the amendments planned by the Minister of Digitisation come into effect.

4.3 Development of the service recipients (consumers) and service providers (businesses) market

The perspective of the service recipient and the service provider

Service recipient – meaning a client who uses a service to address a need. The recipient has become accustomed to online services available instantly, without excessive wait times and without any additional steps. Conducting research on usability of a service and user experience helps improve ease-of-use. A friendly interface, mobile phone accessibility, easy payments, no need to fill in written forms – these are the main features that customers expect from an online service. The process is very simple with regard to paid services that are free from additional transaction-related risk or additional legal requirements. That is why services provided by energy companies, telecommunication operators and, in some cases, insurance companies require the customer to meet with a company representative, or at least sign the contract via a courier. While it is not a major inconvenience, it does cause delays between signing up for a service and initiation of the service.

Service provider – defined as a company that aims to increase the availability of its services, attract more customers, and optimise costs at the same time. Cost optimisation is the most common motivation behind a company initiating the switch from paper-based business processes to electronic ones. The boundary conditions for going paperless are: ensure that customer access to the service is not reduced, and ensure that costs are not higher than those of a paper-based workflow. Typically, long-term profits and benefits outside a single business process are disregarded, including in particular costs of storage, searching, transport and handling in existing branches.

The future development of the market is dependent on awareness, both on the part of the service recipient and service provider. Emerging innovative services certainly affect the competitiveness of the services, which in turn raises awareness among customers and their expectations. Awareness will continue to grow and service providers will have to match new customer expectations. Electronic identification services as well as trust services will see increasing use in this regard, as long as the providers ensure ease-of-use and user-friendliness.

Of course, there are also risks that may affect further development of the market – ones that may completely or temporarily impede the use of electronic services for online transactions. One such risk relates to security in general, understood as the willingness of providers of eID and trust services to manage emerging attacks and combat future attempts at committing fraud through these technologies. Popularisation of electronic identification, electronic signature and trust service solutions will attract the interest of criminals, which is where the accumulated experience of the banking sectors should prove invaluable.

Another risk relates to regulation, which on the one hand has been established at the European level, therefore guaranteeing the stability of regulatory objectives, but it is the national law that specifies guidelines and provides tools for recognition and adoption of trust services within public services. Introduction of legal instruments on the local level may disrupt competition on the market, and thus stunt its future growth.

4.4 Market development

Qualified providers of trust services offer solutions at the highest level of security required by law, required by technical standards, and verified during regular audits. Addressing the business needs of customers is to some extent incompatible with restrictive security requirements, which is why trust service integrators and trust service consultancy firms are of great importance for the development of the market. These operators – familiar with the market expectations, and the capabilities and limitations of qualified services – are able to provide solutions that can satisfy the business requirements of both groups. With consultancy services on business processes of large corporations and digital transformations of such entities, suggestions can be made on the right tools that will be appropriate to the organisational culture of the changing institution. In addition to offering a wide variety of trust services and combining them with other commercial services, integrators are also able to ensure that their solutions fulfil expectations regarding ease-of-use. Integrators can select solutions for SME clients – modular solutions or solutions tailor-made to the sector come to mind – and, for example, present a dedicated offer for an employment agency, a private healthcare provider, a school, a local water supplier or a waste management company, etc.

We have outlined the trust services market, its core services, its potential and its operational environment. This market is currently at a critical juncture. Migration of business processes, consumer processes and administrative processes is in high demand right now, and everything indicates that this demand will continue to grow. The “evidential function” and the regulatory support are also important factors. Commercial and public institutions are looking for methods to fully digitalise their processes and make them available to as many customers as possible. At the same time, end users declare that they would like to see an increased array of online-enabled operations – similar to financial online services, which the customers have embraced in droves.

To secure optimal market development, it is necessary to unify in working together with the regulator to ensure appropriate legal changes are introduced – ones which would grant eID and trust services room to operate in a secure manner. It is also necessary for individual market players to work together and see the potential in collaboration over competition – to work with the regulator, as mentioned, to influence digital service providers, to convince the same providers to use trust services, and to jointly educate the market. As authors of this report, we are convinced that this very project is proof that the market is ready for such a wide cooperation towards a common goal – to build a digital Poland where customers, citizens and entrepreneurs can succeed.

REPORT EXPERT

Aleksander Naganowski, Director
Business Development, Partnerships and Innovation Poland
Mastercard

Digital identity is not some innovation of the future. For many business contractors, it is a pressing need. In a world where all products and services can be ordered through digital outlets, and the easiest way to reach a client is through mobile devices, it is crucial that we possess the means to definitively identify the communicating parties.

That is why MasterCard has taken up the challenge of building a global digital identity standard that ensures that the user is the only true owner of the collected data, rather than the collecting organisation. Restoring trust between parties in the digital world is Mastercard's vision, and we are working towards that vision with partners all around the world.

REPORT EXPERT

Paweł Stosik,
President, Fundacja Polska 5.0

Many business, both Polish and foreign, are noticing similar barriers relating to digital transformation. One of the problems is that some companies do not treat digitalisation as a process, a long-term undertaking. They lack a coherent strategy and lack the people who would oversee such a transformation. An ad hoc digitalisation of individual processes may lead to information chaos, within and outside the company. The second extremely significant barrier, probably the one most often cited by entrepreneurs, lies in the outdated systems and infrastructure. Many of those systems have been built over years, growing more complex with each modification. Modernisation of these systems, which is often crucial for successful digitalisation of the entire company, can be extremely difficult and expensive.

Electronic identification and trust services are one of the most promising tools for comprehensive approach towards addressing these challenges. Our work at Fundacja Polska 5.0 is aimed towards identifying the greatest barriers to digitalisation of processes at the contact point where the citizen, the consumer, and the entrepreneur meet with the state and commercial service providers. A widespread take-up of convenient and secure eID and trust services
may help eliminate these barriers.

REPORT EXPERT

Jon Ølnes,
identity and trust services expert, Signicat

Challenges and solutions for cross-border eID in the EU

There is no such thing as an EU citizenship. All aspects of identity are left to the individual member states, to be handled according to national legislation and culture. Consequently, the formal scope of the electronic identification part of the EU eIDAS regulation had to be limited to non-discriminatory use of electronic identity (eID) across borders for public services. However, the intended effect of eIDAS electronic identification is far wider than the formal scope; in the internal open market, cross-border eID is surely needed for cross-border services of all types.

There is still a way to go for cross-border eID. Actually, many EU member states still struggle either to get a functioning national (in some meaning of that word) eID infrastructure in place, or to obtain a significant number of users of such infrastructures. Leaving the national challenges, the most prominent challenges in cross-border eID in the EU are the following; we return to approaches to solutions at the end of this note:

1. Aligning assurance levels (quality) for eID across member states,
2. Aligning requirements for eID for similar services across member states,
3. Providing unique and persistent identification of persons,
4. Coupling the electronic identification of a person in a member state with the same person's registered identity in another member state.

Regarding challenge 1, an observed effect of eIDAS is that many member states align their national assurance level frameworks with the eIDAS levels "low", "substantial", and "high". Still, there is no automatic equivalence between e.g. "Polish high" and "Norwegian high", unless the eIDs are formally "notified" for cross-border use according to eIDAS. And still some member states have no national assurance level framework (e.g. Germany) or do not align with eIDAS levels.

Requirements for eID (and for use of electronic signatures and other trust services) for specific services vary across member states; such requirements come from sectorial legislation that is usually national. As an example, Norwegian providers of financial services wanted to onboard Swedish customers using Swedish BankID but got a clear "no" answer from the Norwegian supervisory authority. In Norway, eID level "high" is required for onboarding, while Swedish BankID is level "substantial", which is sufficient for onboarding in Sweden. There are ample such examples of diverging requirements, potentially blocking service provision, as for the Norwegian providers in the given example since eID at level "high" is in practice not even available in Sweden (nor in Denmark).

Providing unique identification of natural persons is a problem even at national level in many EU member states, notably those without any national identification number scheme. Close to unique identification is possible by a collection of information attributes of a person, such as name and physical address. The challenge is that this identification is not persistent as these attributes may change over time. And if a member state cannot persistently identify its residents internally, then it surely cannot do so across borders. Even in the presence of a national identification number scheme, unique identification may be difficult since use of such numbers is usually restricted. It is not at all clear that government services in another member state can use a national identification number, not to mention commercial services in another member state.
Regarding challenge 4, consider a Polish citizen being a registered resident of Norway as an example. This person will have both national identification numbers: Polish "PESEL" and Norwegian "fødselsnummer". Norwegian public services require fødselsnummer, meaning that the Pole cannot access such services using a Polish eID unless the PESEL (or other unique identification from the eID) has been previously matched with the fødselsnummer. In cases where the person's unique identification is based on information that may change, or several unique identification methods exist, a person from one country may end up with several identities in another country. If the person signs up for a commercial service once with a Norwegian eID and then with a Polish eID, this will appear as two separate registrations.

So, how do we tackle these challenges? Today only a few eIDs are "eIDAS notified" for cross-border use but the eIDAS assurance level framework is still the only useful benchmark in the EU. A non-notified eID may be assessed against an eIDAS assurance level by preferably an independent conformity assessment. Then, following the logic of eIDAS that an "eIDAS eID" should be accepted on par with national eIDs at the same level, service providers and supervisory authorities should be challenged to accept such foreign eIDs.

Regarding differing eID requirements for the same type of service, this is not easily solved. A service provider must follow the rules of the member state where it is registered. A first step is to enable the service provider to accept "any" eID at sufficient eIDAS assurance level across member states. As one example, Signicat integrates close to 30 different eIDs, making these available through one API. The EU's "eIDAS infrastructure" consisting of interconnected "eIDAS nodes" in each member state may be an alternative but access for commercial service providers is yet unsolved. Further down the road, authorities should be challenged to align service specific eID requirements across the EU.

When a person's real, national identity is needed, which is the case e.g. for financial services, a "primer" must be available to prove the identity. Signicat's experience is that multiple mechanisms are necessary depending on available means in different countries. Using an existing eID of sufficient level and providing the needed informa-

tion is by far the easiest way; then this eID may also continue to be used for authentication if desired. Use of physical identity documents is the fallback alternative, either by personal appearance or by remote reading by video, photo or, preferably, by information from the document's NFC chip. An advanced/qualified signature supported by an existing certificate providing assessed identity information is also possible. Unless an existing eID can be used, a new eID must be issued for future authentication. This eID need not be national nor carry any national identification attributes; it can be the same for all users across countries. Since almost all persons possess smart phones supporting apps and biometrics, issuing a service specific eID either in the form of a dedicated app or integrated into service apps increasingly becomes viable. Signicat MobileID is one possible foundation for such service specific eIDs. The national problems of persistent unique identification however remain.

Mapping different (national) identities for the same person is targeted by some initiatives. The Nordic and Baltic countries co-operate to create a common "eID region" where identities can be translated by entering national identification numbers from other countries in the national population registers. The EU's EESSI (Electronic Exchange of Social Security Information) includes identity mapping to ensure co-ordination of benefits across member states. For commercial service providers, the problem persists. Advanced eID and identity management solutions can tackle some of the problems by mapping several national identities into one service specific identity.

Glossary

'electronic identification (eID)'	means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
'electronic identification means'	means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
'person identification data'	means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
'electronic identification scheme'	means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
'authentication'	means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
'relying party'	means a natural or legal person that relies upon an electronic identification or a trust service;
'public sector body'	'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
'body governed by public law'	means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council;
'signatory'	means a natural person who creates an electronic signature;
'electronic signature'	means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
'advanced electronic signature'	means an electronic signature which meets the requirements set out in Article 26;
'qualified electronic signature'	means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

'electronic signature creation data'	means unique data which is used by the signatory to create an electronic signature;
'certificate for electronic signature'	means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
'qualified certificate for electronic signature'	means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
'trust service'	means an electronic service normally provided for remuneration which consists of: a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or b) the creation, verification and validation of certificates for website authentication; or c) the preservation of electronic signatures, seals or certificates related to those services;
'qualified trust service'	means a trust service that meets the applicable requirements laid down in this Regulation;
'conformity assessment body'	means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
'trust service provider'	means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
'qualified trust service provider'	means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
'product'	means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
'electronic signature creation device'	means configured software or hardware used to create an electronic signature;
'qualified electronic signature creation device'	means an electronic signature creation device that meets the requirements laid down in Annex II;
'creator of a seal'	means a legal person who creates an electronic seal;
'electronic seal'	means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
'advanced electronic seal'	means an electronic seal, which meets the requirements set out in Article 36;
'qualified electronic seal'	means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

‘electronic seal creation data’	means unique data, which is used by the creator of the electronic seal to create an electronic seal;
‘certificate for electronic seal’	means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
‘qualified certificate for electronic seal’	means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;
‘electronic seal creation device’	means configured software or hardware used to create an electronic seal;
‘qualified electronic seal creation device’	means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;
‘electronic time stamp’	means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
‘qualified electronic time stamp’	means an electronic time stamp which meets the requirements laid down in Article 42;
‘electronic document’	means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
‘electronic registered delivery service’	means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
‘qualified electronic registered delivery service’	means an electronic registered delivery service which meets the requirements laid down in Article 44;
‘certificate for website authentication’	means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
‘qualified certificate for website authentication’	means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
‘validation data’	means data that is used to validate an electronic signature or an electronic seal;
‘validation’	means the process of verifying and confirming that an electronic signature or a seal is valid.

OBSERWATORIUM . BIZ

Digital Transformation of Companies

Strategy & Benchmarking

Integration of Trust Services and eID

Ergonomics of Digital Processes

REPORT AUTHORS

Miłosz Brakoniecki –
Board Member, Obserwatorium.biz Sp. z o.o.

Michał Tabor –
Board Member, Obserwatorium.biz Sp. z o.o.

Marcin Wolski –
Expert, Obserwatorium.biz sp. z o.o.

Marcin Żywicki –
Analyst, Obserwatorium.biz sp. z o.o.

Layout: Szymon Brakoniecki
Proofreading: Anna Mróz
Translation: Zespół Tłumaczy Przysięgłych w Olsztynie

main patron

EFPE

scientific partner

C@ntrum
Prawnych Problemów Techniki i Nowych Technologii

social partner

POLSKA 5.0

partner

KIR

partner

asseco
DATA SYSTEMS

partner

SIGNICAT

partner

go.eIDAS

honorary patron

PIIT

honorary patron

MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII

Methodology of the report

This report – "Paperless Business. Commercialisation of eID and Trust Services in Poland and Europe" – has been prepared based on the knowledge of the partners and associates of Obserwatorium.biz, and on their analyses of the Polish and foreign electronic identification and trust services markets, including the use of such services in business and public administration. The report also draws upon CAWI surveys (i.e. web questionnaires) conducted in Q1 2019 – the sample group comprised persons directly involved in the eID and trust services market. The report includes statements by members of the following organisations: Krajowa Izba Rozliczeniowa S.A., Asseco Data Systems S.A., Kancelaria Prawna Szostek & Bar, Poczta Polska S.A., Rachuneo, Sighnero, Polska Izba Informatyki i Telekomunikacji.

Legal disclaimer

Opinions found in this report have been expressed based on the knowledge gained from market research and the authors' experience. The authors do not take responsibility for decisions based on opinions expressed in the "Paperless Business. Commercialisation of eID and Trust Services in Poland and Europe" report.