ID4D
IDENTIFICATION FOR DEVELOPMENT

Moldova
Mobile ID Case Study

WORLD BANK GROUP

Contents

About ID4D

The World Bank Group's Identification for Development (ID4D) initiative leverages global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals (SDGs). It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal aspects, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have secure, verifiable, and officially recognized identification. ID4D makes this happen through its three pillars of work:

- Thought leadership and analytics to generate evidence and fill knowledge gaps;
- Global platforms and convening to amplify good practices, collaborate, and raise awareness; and
- Country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible through support from the World Bank Group, Bill & Melinda Gates Foundation, Omidyar Network, and the Australian government.

To find out more about ID4D, visit id4d.worldbank.org

Acknowledgments

This Case Study was prepared in 2018 by Vlad Manoil, Chief Reengineering Officer of the e-Governance Agency of Moldova, and Iurie Turcanu, Chief Digital Officer of the e-Governance Agency of Moldova.

The case study benefited from guidance from Luda Bujoreanu (Senior Program Officer, ID4D, WB) and inputs received from peer reviewers, including Stela Mocan (Lead IT Officer, Business Solutions, ITS, WB), Yiannis Theodorou (Director of Policy & Advocacy, Digital Identity and Mobile for Humanitarian Innovation, GSMA), Natasha Beschorner (Senior ICT Policy Specialist, Digital Development Global Practice, WB), and Anna Zita Metz (Analyst, ID4D).

Abbreviations

API	Application Program Interface
ARPU	Average revenue per user
CA	Certification Authority
CD-ROM	Compact Disc Read-Only Memory
CTS	Center for Special Telecommunications
DVCS	Data Validation and Certification Server
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication, and Trust Services
FSI	FiscServInform
G2B	Government to Business
G2C	Government to Citizen
GeT	Governance e-Transformation Project
GoM	Government of Moldova
HSM	Hardware Security Module
ICT	Information and Communication Technology
IDNO	Identification Number of Organizations
IDNP	Identification Number of Persons
ISP	Internet Service Provider
MeID	Mobile Electronic Identification
MNO	Mobile Network Operator
MSSP	Managed Security Service Provider
OCSP	Online Certificate Status Protocol
OTA	Over the air
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
SIM	Subscriber Identity Module

SIS	Security and Intelligence Service
SMS	Short Message Service
SRLE	State Register and Legal Entities
SRP	State Register of Population
TAN	Transaction Authentication Number
TSP	Time Stamping Service

Executive Summary

The Republic of Moldova was among the first countries in the world to implement Mobile eID, which has been implemented through the innovative Public-Private Partnership (PPP) model. In recognition of Moldova embracing mobile technologies as an opportunity to tap the potential of mobile phones to improve government initiatives, the government of Moldova was awarded the *Best mGovernment Award* by the GSMA during the 2013 Mobile World Congress in Barcelona.[1]

The concept of Mobile eID, also known as mobile signature, works as an ID in the virtual world, allowing users to authenticate themselves in cyberspace, with the aim to prove their identity with the help of a cell phone or electronically sign a legally-binding transaction or document. For the regular users, the advantage of mobile eID lies in its simplicity, since no separate card reader or drivers are needed, as the phone itself already performs these functions.

Implementation of Mobile eID in Moldova was part of a larger digital transformation initiative supported by a US$20 million World Bank–funded loan as part of Governance eTransformation Project (GeT),[2] and as such, it benefited from increased political support. Moreover, the approval by the government of Moldova of the strategic e-Transformation program further paved the way for eID implementation, by expressly stating that mobile electronic identity is "a means to ensure data integrity and security in eservice delivery and financial transactions."

Its implementation started in 2011 as part of a Governance eTransformation program. However, due to limited financial resources, the government reached out to mobile operators to check the willingness of Mobile Network Operators (MNOs) to invest in an innovative Mobile eID PPP solution.

The implementation of Mobile eID through a PPP was transformational, allowing for the digitization of interactions between the government and citizens, residents and businesses. It allowed for mainstreaming the use of electronic signatures by making it user friendly and affordable. Citizens are now able to obtain a Mobile eID in about 15 minutes, in 700+ offices of mobile operators across the country free of charge, by only presenting a national ID card or a permanent resident card to help the mobile operator validate the person's identity against the State Population Registry.

Mobile ID implementation took roughly 18 months. The first 12 months were devoted to reaching out to mobile operators, building consensus around a possible PPP model and signing the agreement between the eGovernment Center, as a coordinating body for e-governance and digital transformation processes in the country, the state-owned enterprise Center for Special Telecommunication as certification authority, and two of the three mobile operators in Moldova—Orange Moldova, part of the Orange Group, and Moldcell, part of the Telia Sonera group—as registration authorities.

Implementation of the technical solution took another 6 months due to the strong commitment of the government team to deliver the project and the agility and commitment of participating mobile network operators. Since most of the infrastructure investment was made by the private partners, the government did not need to conduct any procurements. The government was able to leverage the existing Public Key Infrastructure (PKI), while letting the private sector procure what they thought was the most appropriate

1 https://www.gsma.com/newsroom/press-release/gsma-announces-winners-of-the-2013-global-mobile-awards/
2 http://projects.worldbank.org/P121231/governance-etransformation-project?lang=en

technical solution for providing a reliable, cost-efficient, and rapid platform for Mobile Electronic Identification (MeID) deployment.

This case study provides background information about Moldova's digital transformation journey and unveils the details of Mobile eID implementation and key success factors in terms of infrastructure and institutional arrangements, as well as a legal and regulatory environment. It also highlights the impact of Mobile eID on the overall digital transformation of Moldovan government and particularly, the role that mobile ID played in improving e-service delivery in key sectors.

The case study also sheds light on the partnership between the eGovernment Center, as a coordinating body for e-governance and digital transformation processes in the country, the state-owned enterprise Center for Special Telecommunication as certification authority and two of three mobile operators in Moldova—Orange Moldova, part of the Orange Group, and Moldcell, part of the Telia Sonera group—as registration authorities. It provides insights into motivation of the parties, technical architecture, commercial models, investments, implementation timeframes, and the impact on electronic services, and also articulates lessons learned which might be of an interest to other countries.

Country Context

Moldova is a small lower-middle-income economy, located in Eastern Europe, northeast of Romania (see Map 1). Although it is the second poorest country in Europe, Moldova has made significant progress in reducing poverty and promoting inclusive growth since the early 2000s.

European integration has anchored the government's policy reform agenda, but many reforms have yet to materialize. A vulnerable political system, polarized society, adverse external environment, and skills mismatch in the labor market, as well as climate-related shocks, remain Moldova's biggest economic challenges even today.

A large proportion of Moldovans (as many as 40 percent by some estimates) work and live abroad, primarily in Europe. The government needed to find a way to better serve its people, including those living outside of its borders and has embarked on an e-transformation journey to be able to deliver services electronically and remotely.

Map 1. Country of Moldova

In 2011 there were three mobile operators on the market (Orange Moldova, Moldcell, and Unite). Mobile phone penetration was 104 percent, and therefore, a Mobile eID solution seemed a natural choice for the government. Other relevant telecom data is in Table 1.

Table 1. Moldova Key Telecommunication Market Indicators

Indicator	2011[3]	2017[4]	Change
Mobile communications			
Subscribers	3,714,965	4,459,999	+745,034
Penetration	104.34%	125.60%	+21.26 percentage points
Mobile Internet			
Subscribers	124,813	2,430,078	+2,305,265
Penetration	3.5%	68.44%	+64.94 percentage points
Dedicated mobile Internet traffic (TB)	6,168	43,726	+37,558
Fixed Internet			
Subscribers	355,099	584,330	+229,231
Penetration	10.0%	16.5%	+6.5 percentage points
Total external Internet capacity (Gbps)	122.74	356.40	+233.66

3 Evolution of telecommunication markets. Report for 2011 (http://anrceti.md/files/filefield/Raport%20ANRCETI%20(rom)%202011.pdf)

4 Evolution of telecommunication markets. Report for 2017 (http://anrceti.md/files/filefield/2017_EvPiata_Raport.pdf)

1. Moldova's Digital Transformation Agenda

In 2011, the government of Moldova embarked on a strategic governance modernization program,[5] aiming to radically transform delivery of public services using information and communications technologies (ICT). This was supported by the "Governance eTransformation" project, financed by the World Bank in the amount of US$20 million International Development Credit (IDA) credit. An e-Governance Agency was set up and appointed as the implementation agency for this ambitious, nationwide e-transformation program.

Even today, Moldova's digital agenda continues to revolve around 13 core priorities, such as adoption of cloud computing and consolidation of digital infrastructures, data exchange and interoperability, information security, and others, with digitization of public services being at the very core.

In 2011 Moldova was well positioned to capitalize on a few positive factors, such as:

- Seven major Internet Service Providers (ISPs) covering the entire country
- Broadband access covering 92 percent of the territory
- High mobile network (penetration of 104.34 percent)
- 4G covering 95 percent of the territory
- Average computer literacy of the population
- Well-established foundations ID system
- Existence of PKI
- New government with an ambition to leapfrog and improve service delivery

The government's e-Transformation Strategy laid down the foundation for an ambitious program, which entailed a complex reform of 587 public services for citizens and businesses and adoption of 21st century e-government practices and tools, with the aim to cut bureaucracy, corruption, administrative costs, inefficiency, and lack of productivity. Broadening the availability of and access to e-services was also necessary to address the needs of a large share of the adult population who continued to work abroad and were thus unable to access government services that required them to be physically present in-country.

The government has set the objective to have all public services digitized and accessible remotely by both individuals and businesses. Public authorities, with support of development partners and the eGovernance Center, started to develop or modernize public services, making them more accessible, user friendly, and trustful. The government needed to find a solution for obtaining the e-signature which resulted in very low adoption rates because of the following:

- Cumbersome process to obtain e-signature
- High cost of e-signature
- Only one location in the country where one could obtain e-signature

In this context, the deployment of the Mobile eID infrastructure was critical for streamlining the delivery of public services, including to segments of the population who left the country to work abroad. Moldova's

5 http://lex.justice.md/md/340301/

Mobile eID solution added speed, privacy, affordability, accessibility, and transparency to numerous government services for citizens and businesses, including online applications and copies of official documents.

Nowadays, even the services that require a higher level of assurance can be delivered via a mobile device using electronic signatures, thanks to the Mobile eID solution. For example, individuals and businesses can file their taxes online, submit e-reports, and request e-services.

By mid-2018, the total number of active eID users (i.e., having a device with a valid certificate) was about 300,000, out of which about 100,000 were Mobile eID users. The average monthly number of esignatures produced via MSign was about 2 million, more than half of which were used for tax declarations and e-reporting.

2. Building Blocks as Critical Success Factors

Existing infrastructure

Moldova's success with Mobile eID did not happen overnight. However, the country had a few building blocks in place, which allowed for innovation in the eID field, including:

- **A robust, high coverage foundational ID system:** Moldova's State Register of Population (SRP) was established in 1993 and assigns each citizen at birth a 13-digit personal identification number referred to as an Identification Number of Persons (IDNP). Virtually the entire population of Moldova is registered in the SRP, except for data from the breakaway region of Transnistria.[6] SRP is the core data source containing identification information and serves as the primary data source for numerous other registers and systems.
- **A robust business registry:** Moldova's State Register and Legal Entities (SRLE) was founded in 2002 and stores data about commercial entities, except individual entrepreneurs and farms. Legal entities are also assigned a unique 13-digit identifier called Identification Number of Organizations (IDNO). Before the establishment of SRLE, the companies were assigned taxpayer identification numbers, which were later replaced with IDNOs.
- **A national PKI infrastructure** was established in Moldova in September 2005 following the approval of the law on digital signature and electronic documents. The government appointed the Security and Intelligence Service as the root certification authority (CA). In September 2006, the Center for Special Telecommunications (now the Service for Information Technology and Cyber Security or SITCS) launched the first sub-root certification authority, providing digital signature services, including qualified signatures for government, businesses, and citizens. Currently SITCS is the only authorized certification authority, following the consolidation of three state-owned CAs in August 2017. However, the list of registration authorities[7] is larger and includes the Center for IT in Finance, Agency for Public Services, Orange, and Moldcell. Annex 2 provides more details on the evolution and current state of Moldova PKI.

Enabling legal and regulatory framework

Mobile eID would not have been possible if it wasn't for a favorable legal and regulatory environment, which is evolving over the years and adapting to current and future needs.

The law on electronic document and digital signatures was approved in 2004[8] and laid the foundation for the exchange of electronic documents and digital signatures. It also gave electronic documents the same legal power as paper documents. In 2014, a new **law on electronic signatures and electronic**

6 Transnistria is a breakaway region of Moldova in which ethnic Russians and Ukrainians together outnumber ethnic Moldovans. It has had de facto independence since a brief civil conflict in 1992 but is internationally recognized as part of Moldova. (https://freedomhouse.org/report/freedom-world/2017/transnistria)

7 A Registration Authority is an authority in a network that verifies user requests for a digital certificate and tells the Certificate Authority to issue it.

8 http://lex.justice.md/md/313061/

documents was approved,[9] which created the framework for applying Directive no. 1999/93/EC of the European Union.[10] Further efforts are made to harmonize the current law with provisions of EU's Electronic Identification, Authentication, and Trust Services (eIDAS) Regulation 910/2014,[11] and an update to the law is expected in 2019.

Other relevant legal acts include the government Decision no. 320 of 28.03.2006 on approval of a **regulation regarding the use of digital signatures in electronic documents of public authorities,**[12] and Order of the Security and Intelligence Service No. 69 of 15.07.2016 regarding the approval of **Technical norms in the field of advanced qualified electronic signatures.**[13] A comprehensive list of applicable laws and technical standards is presented in Annex 1.

The present redaction of the law distinguishes between simple, advanced unqualified, and advanced qualified electronic signatures. Table 2 outlines the differences between them.

Table 2. Types of Electronic Signatures

	Simple electronic signature	Advanced unqualified electronic signature	Advanced qualified electronic signature
Used for authentication (identity proof) in cyberspace	x	x	x
Exclusively points to signatory		x	x
Allows for identification of signatory		x	x
Is created using methods exclusively controlled by the signatory		x	x
Is bound to the data it reports to, so as to detect subsequent changes to the data		x	x
Is based on a qualified public key certificate issued by an accredited provider of certification services			x
Is created using a secure signature creation device and can be securely verified			x

Political will

Implementation of Mobile eID in Moldova was part of a larger digital transformation initiative supported by a US$20 million World Bank funded loan as part of Governance eTransformation Project (GeT)[14] and as such, it benefited from increased political support. Moreover, the approval by the government of Moldova of the strategic e-Transformation program further paved the way for eID implementation, by expressly

9 http://lex.justice.md/md/353612/
10 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN
11 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
12 http://lex.justice.md/md/315579/
13 http://lex.justice.md/md/365884/
14 http://projects.worldbank.org/P121231/governance-etransformation-project?lang=en

stating that mobile electronic identity is “a means to ensure data integrity and security in eservice delivery and financial transactions.”

With the introduction of mobile eID, 95 percent of the citizens of Moldova[15] instantly gained access to a simple way of signing documents and transactions with no technical knowledge required.

Then Prime Minister Filat, a driver of the wider e-Transformaiton agenda, was the first person to officially sign an official document using MeID (Figure 1), the Directive 80-d of September 14, 2012, on increasing the use of mobile signatures as part of the electronic signature infrastructure.[16]

Figure 1. Mobile eID Launching Ceremony, the First Official Document Signed Using Mobile Signature and Project Logos

15 The cumulative market share of the two participating MNOs (Orange and Moldcell) is circa 95 percent.
16 http://lex.justice.md/md/344825/

3. Mobile eID Implementation: An Innovative PPP Approach

Even though in 2011 Moldova's PKI was fully functional, and citizens could potentially use e-signatures, there were several key factors that made the government seek alternative eID devices and channels:

- **Low uptake** of the existing channels (smart cards), before Mobile eID was introduced;
- **Insufficient mobility and portability** of the existing devices, as card readers were needed along with the smart cards and were not supported on platforms such as tablets and smartphones;
- **High prices** for electronic signature kits, while offering **little value for the money;**
- **Steep learning curve,** as existing devices and channels required advanced technical skills;
- **Few electronic services** requiring the use of electronic signatures; and
- **Low outreach,** with only one issuing office in the capital city of Moldova where one could obtain a device enabled for electronic signatures.

As a result, citizens preferred to apply for the services in person rather than applying online with an electronic signature. It was clear that an alternative solution for provision of e-signatures was needed.

Implementation model: public-private partnership

Prior to developing the Mobile eID solution, the government of Moldova undertook an extensive analysis of the options available. The World Bank played a significant role in identifying the right solutions and has facilitated access to cutting-edge expertise in this area, namely through consultations with a high-level expert practitioners network (known as HELP).

When designing the MeID solution, the following key criteria were considered by the government and private partners:

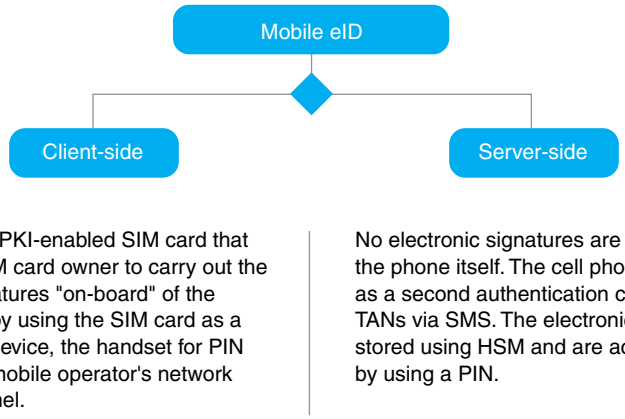
- Implementation and maintenance costs;
- Implementation timeframe;
- Degree of accessibility for the end users in terms of usability and costs; and
- Degree of administrative usability during enrollment, validation, and issuance stages.

In the end, the government had to choose from two distinct alternatives as presented in Figure 2.

A *client-side model* is used by some countries like Sweden, Finland, and Estonia, while a serverside model is used by the Austrian federal government. Annex 4 offers more details on the differences between the two options in terms of user registration, authentication, and the e-signing process.

After a thorough analysis and discussions with all stakeholders both from public and private sectors, the government chose to deploy the client-side MeID option. One of the key arguments in favor of this option was the openness of MNOs to invest in an innovative product that could also help them diversify and consolidate their user base. Commercial banks also contributed to this decision as they articulated their need for secure authentication and e-signature instruments, while expressing reluctance to embrace a solution in which the private keys were stored in government Hardware Security Modules (HSMs).

Figure 2. Mobile eID Alternatives



Partnership with mobile network operators unpacked

To implement the Mobile eID in Moldova, a partnership agreement was signed between the:

- eGovernment Center, as a **coordinating body** for e-governance and digital transformation processes in the country;
- The state-owned enterprise Center for Special Telecommunication as **certification authority (CA);** and
- Two of three mobile operators in Moldova: Orange Moldova, part of the Orange Group, and Moldcell, part of the Telia Sonera group, as **registration authorities (RA).**

The main responsibilities between the government and MNOs, as set out by government regulation,[17] are split according to Table 3.

Table 3. Split of Responsibilities between RA and CA in the Context of MeID

	Government (CA role)	MNOs (RA role)
Registration/ enrollment	■ Registration in and maintenance of foundational ID systems and registries and issuance of ID credentials ■ Issuance of qualified electronic signature certificates ■ Provision of automated user data validation interface with the SRP	■ User identification, validation and registration (based on government-issued ID credentials) ■ Issuance of PKI-enabled SIM card and service activation
Operations	■ Provision of signature validation service ■ Provision of time-stamping service	■ Data transport over mobile networks (OTA platform) ■ Billing and invoicing ■ Customer support

17 https://pki.cts.md/fileadmin/templates/pki_files/about_legislatie/Regulament_privind_functionarea_centrului_de_inregistrari_al_CCCP.pdf

End-user data are stored in the country's population registry; against which mobile operators check customer data to enroll them. The mobile operators have no direct access to the registry or other citizen data; the provided Application Program Interface (API) validates user data from the ID card to prevent fraud and identity theft. Mobile operators log customers' use of mobile signatures for billing purposes, but no information regarding the nature of services for which the mobile signatures were used.

According to the partnership agreement, the mobile operators were responsible for providing the technical infrastructure required for Mobile eID, which amounted to circa EUR 400,000 for each MNO, mostly for additional hardware and increasing network strength. The government, in its turn, was responsible for integrating the infrastructure on the MNOs side with existing government PKI, which amounted to approximately US$30,000. The revenue from mobile signature transactions is also split between MNOs and the government, with 85 percent going to MNOs to cover their initial investment and operating costs and 15% being directed for the maintenance of government PKI.

Mobile operators charge end users a fee for the use of mobile signatures, and the pricing structure can vary depending on specific contract and bundling models, much like airtime, data usage, or text messaging. For example, mobile subscribers can opt for a *pay-per-use model,* which is most suitable for those who are rarely in need of this service, as well as for bundles ranging from 10 to 1,000 transactions. Information about current prices and offers can be found on the websites of participating MNOs.[18]

Win-win-win scenario

The implementation of mobile ID through a PPP arrangement was a "win-win-win" situation for all:

- Citizens and businesses obtained an affordable, hassle-free way to apply for and use qualified digital signatures;
- Mobile operators were able to offer a new innovative service to their subscribers and increase customer loyalty; and
- Government obtained a new electronic signature channel with delivery points already present throughout the country and built a base for an inclusive digital transformation.

Technical implementation of eID

On the MNO end, the implementation is based on ETSI TS 102 204 technical specifications for mobile signatures.[19] On the other end, to simplify integration of MeID with government e-services, the e-Government Center has developed two reusable platforms for authentication (MPass) and electronic signing (MSign). Overall, the solution architecture is presented in Figure 3.

While the technical implementation of MeID would have been sufficient without MPass and MSign services (offering only the SPKI interface or even access to MSSP interfaces), these platforms play a key role in simplifying integration with third-party e-services and stimulating adoption.

Even though Mobile eID is simple from the end-user perspective, behind the scenes, the information flow is more complex. Figure 4 illustrates an end-to-end scenario of accessing a service using mobile signature.

18 https://www.orange.md/?p=1&c=8&sc=87&s=871 and https://moldcell.md/rom/servicii/utile/semn%C4%83tura-mobil%C4%83-1
19 https://www.etsi.org/deliver/etsi_ts/102200_102299/102204/01.01.04_60/ts_102204v010104p.pdf

Figure 3. Moldovan Mobile eID Architecture

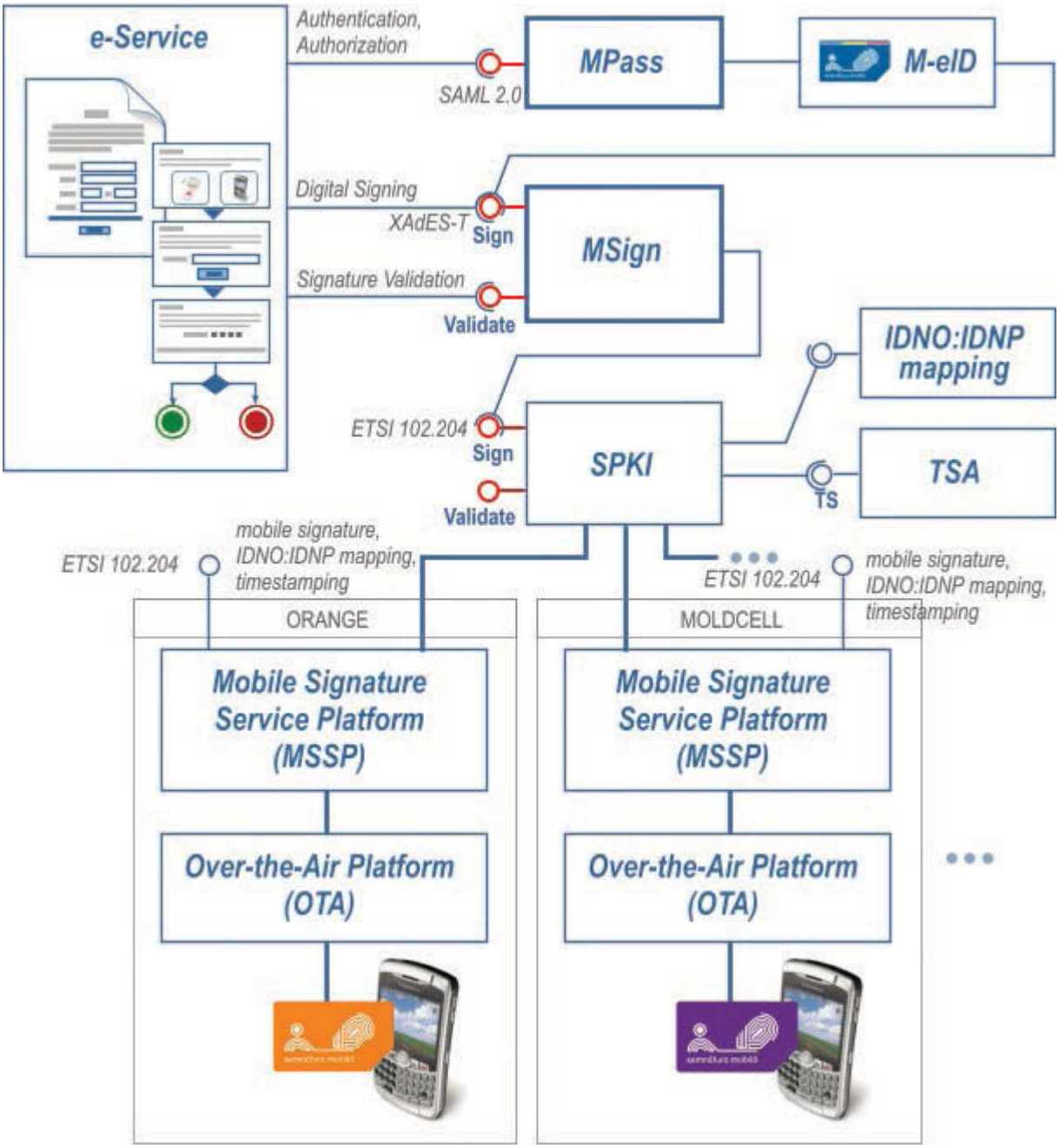
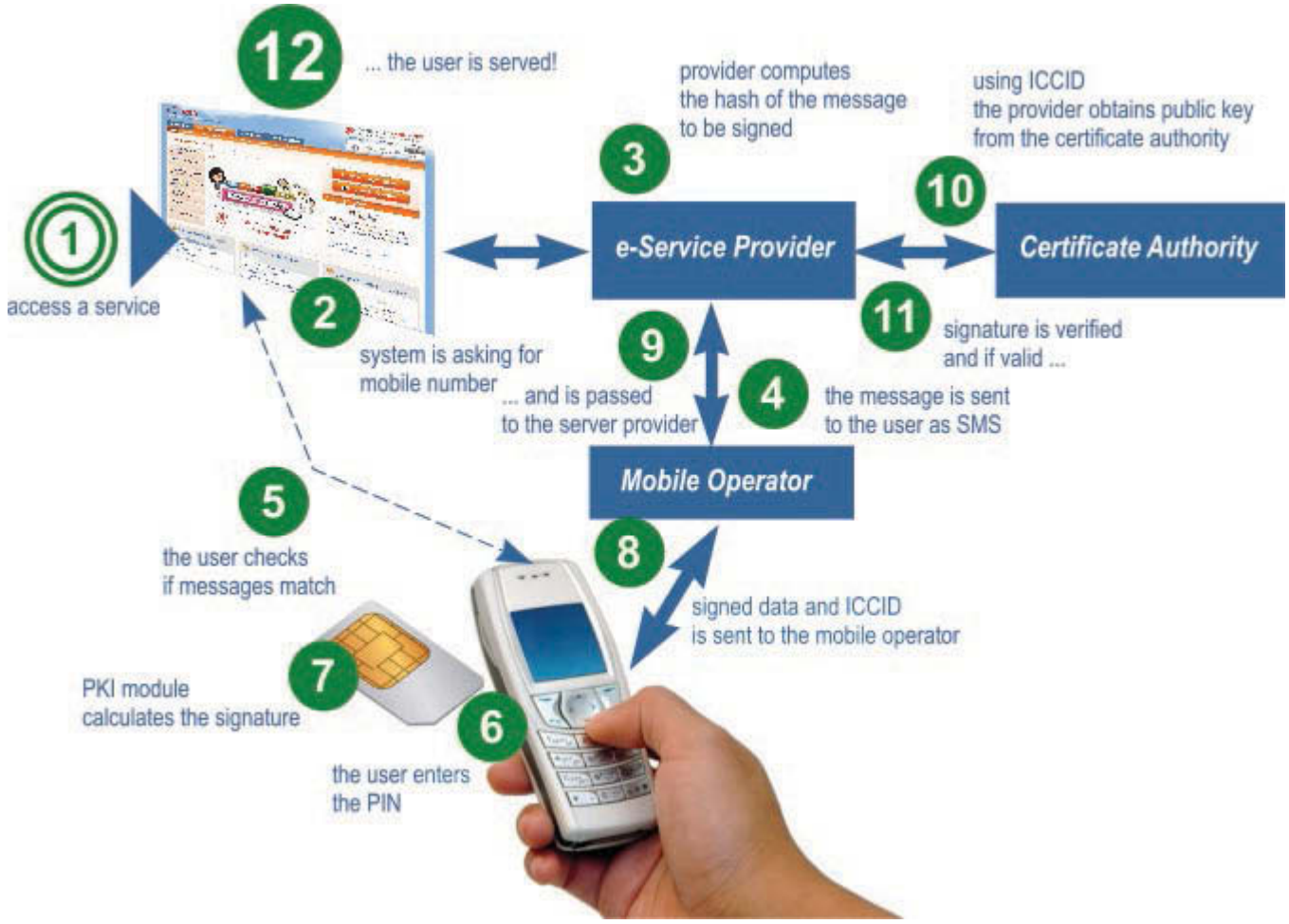


Figure 4. Mobile Signature Flow



4. The eID Evolution: Devices

Electronic signatures are used by most transactional public services, as well as in several private services, to authenticate individuals and businesses when accessing digital services and transactions and when signing digital documents. The electronic signatures can be used for both G2C and G2B scenarios as there are no separate certificates for legal entities.

Devices for eID transactions

Moldovan citizens and residents can obtain an unlimited number of advanced qualified electronic signatures on several types of devices, according to their preference, and they all point to the same physical identity (see Figure 5 for details).

Figure 5. Tools Available for Advanced Qualified Electronic Signature

Smart cards

The first cryptographic smart cards were introduced in 2006, and they were the first secure signature device available to Moldovan citizens. The smart card esignature kit includes the card, cryptographic keys, and the card reader. After the introduction of USB tokens, the smart cards are issued to citizens and businesses only on demand. Currently, the smart cards are mostly used as multipurpose personalized

access cards for government employees to (i) help identify government employees, (ii) allow access to government facilities, (iii) allow government employees to be identified within the Civil Service Registry, and (iv) electronically sign documents and records.

USB tokens

First introduced in 2011, the USB tokens are devices which allow secure storage of the public key certificate for authentication and electronic signature. They combine the security of certificate-based technology with the simplicity of a plug-and-play USB interface and offer a safe environment for electronic transactions that prevent change and manipulation. The USB tokens are mostly used by the businesses and government employees who need to sign a lot of documents from a variety of locations and devices.

Mobile eID

In 2011, the eGovernment Center partnered with the main mobile network operators and the Center for Special Telecommunications to implement the mobile eID using a client-side model, whereby the private key is stored on a special crypto processor–enabled SIM card. The onboarding process is very simple and includes three steps: (i) validation of identity of the person against the State Register of Population, based on a valid national ID or permanent resident card; (ii) replacement of the simple SIM card with a PKI-enabled one; and (iii) generating the private and public key pair on the SIM by the mobile network operator and setting up the PIN code by the user.

The validity of the certificates on the SIM cards is currently one year, and certificates can be renewed remotely (online or via SMS) without the need to replace SIM cards or visit MNO offices, provided the previous certificate has not expired and can be used to electronically sign the renewal request. Mobile eIDs are equally used by citizens and small businesses who do not need to sign many documents at once.

Electronic ID cards

Starting in May 2014, the government of Moldova started issuing ICAO-compliant electronic identity cards (eID) of ID-I format, made of polycarbonate. Moldovan eIDs are built on a modern contactless Near-Field Communication (NFC) interface and comply with *ISO/IEC 14443*. However, issuing of eID cards is optional and the citizens can opt for a cheaper ID card with no electronic signature means. The validity of the private key certificate on the eID is one year and certificate renewal is free of charge, but can only be performed in person at the multifunctional service provision centers.

All devices correspond to the highest level of assurance according to provisions of ISO 29115 and eIDAS. This entails very strong authentication mechanisms and in-person registration with verification, which translates to the lowest levels of risk.

Annex 3 provides more details about the technical specifications of these electronic signature devices.

5. Moving from Paper to Digital: Prominent eID Use Cases

There are three notable cases of use of electronic identity in the public sector, which changed the modus operandi of public and private organizations, significantly improved the quality of associated processes and data, and indirectly contributed to a better adoption of electronic identity.

Electronic tax filing and invoicing

Until 2009, all fiscal reporting was paper based using typical printed forms. The forms were filled in by accountants of reporting organizations and transmitted to Tax Authority offices. Those, in turn, manually verified the completeness and accuracy of the provided information and used it for further analysis and other fiscal operations. Being paper based, this process was too costly and inefficient. The Tax Authority made several attempts to streamline the process, for example, by optimizing the number of collection points or using bar codes on tax documents, etc., but the impact of these reforms was limited.

The problem was solved with electronic submission of tax reports and declarations, which from January 2011 became mandatory for all registered businesses and the preferred option for individuals. One of the core challenges was to uniquely identify taxpayers. In the first version of e-declaration, the authority used simple username and password credentials to authenticate users, but this authentication method proved not sufficiently robust for the level of assurance required for this type of transaction. Instead, the Tax Authority introduced the use of electronic IDs for its systems, starting with advanced unqualified digital certificates and moving to legally binding advanced qualified digital certificates. The transition from simple authentication to advanced qualified signature was made in stages and was accompanied with an ample communication campaign, making the process smooth.

Building on the success with tax e-declaration and e-reporting, in 2015 the Tax Authority introduced electronic fiscal invoices, where the old process of using paper-based invoices was replaced by electronically generated and signed documents, thus automating the transaction between seller, buyer, and the transporter. Combined with interagency data exchange, this has contributed to gradual reduction of reporting obligations since transactions are automatically recorded in the Tax Authority's information systems.

Electronic reporting of employment and payment transactions

The National House of Social Insurance (NHSI), which followed the example of the Tax Authority, started to collect reports on employment and payments to the Social Insurance Fund in electronic form using the eID. NCSI made this reporting obligation mandatory in electronic form starting with January 2017. This change was well received by the business community since it was already prepared for it, and a notable increase in use of eIDs followed this reform.

Electronic submission of civil servants' asset and interest declarations

Starting with January 2018, the National Integrity Agency (NIA) began accepting declarations from more than 70,000 civil servants in electronic form. According to national legislation, each civil servant must submit yearly declarations of assets and interests. Until 2018, these declarations were collected manually within organizations using paper-based forms and then transported to NIA for manual processing. The processing involved a lot of effort, including scanning, indexing, masking personal data, and publishing these declarations. Since 2018, NIA collects all documents exclusively in electronic form, minimizing the need for manual processing and dramatically reducing the cost of processing and publishing times for the declarations. The declarations are digitally signed by civil servants with signature kits offered to them free of charge by the government.

Private sector adoption of electronic signatures

Following the growing use of eIDs in the public sector, different professional communities and associations, such as prosecutors, bailiffs, notaries, insurance officers, traders, and brokers expressed interest in leveraging the electronic IDs in their day-to-day activities, thus improving their performance and bringing more consistency to transactions.

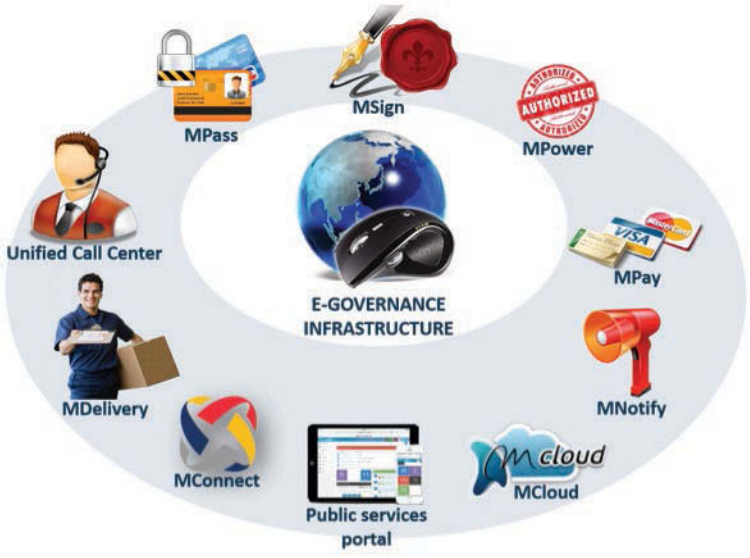
There are several examples where the private sector uses electronic identification for commercial services. The leaders are the banks and microfinance organizations, which rely on electronically signed transactions when offering loans to their clients remotely. Some banks have integrated their banking systems with signing APIs provided by the government while others used APIs provided by individual mobile operators offering Mobile eID.

6. Moldova's eID Ecosystem

Using electronic identity in the context of e-service provision offers many benefits, the most important of them being the trust created between service provider and service user (consumer).

To ensure this trust and offer electronic service providers a simplified and common way to integrate strong authentication and digital signature functionality into their services, the Moldovan eGovernance Agency developed a suite of shared platforms, notably MPass (offering strong authentication and single sign-on functionality across Government information systems and e-services) and MSign (used to electronically sign documents and records and validate electronic signatures), depicted on Figure 6 below:

Figure 6. E-Governance Infrastructure



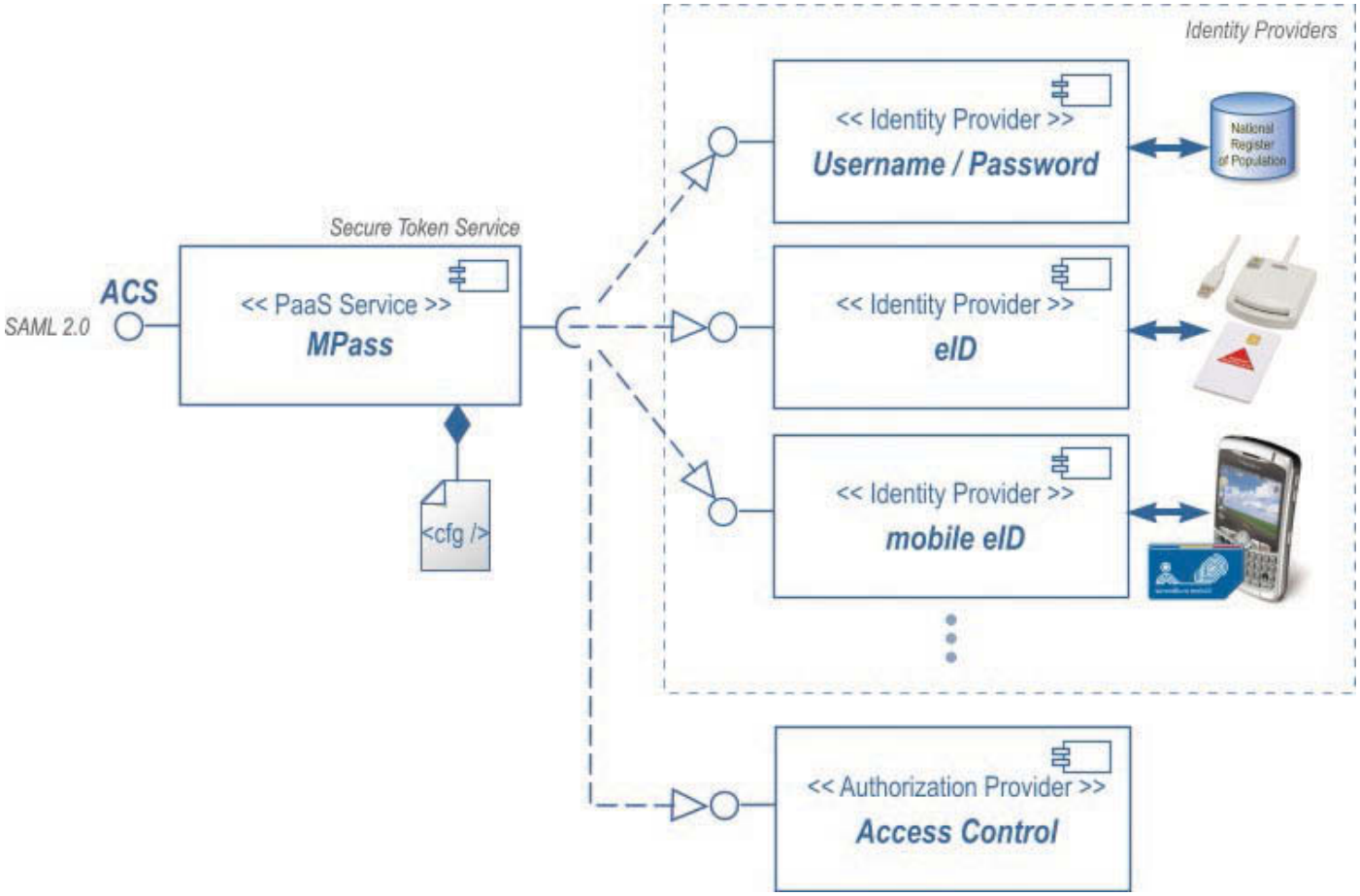
MPass—authentication, authorization and single sign-on service

MPass is a centralized service, which provides authentication and authorization functionality for integrated services. In fact, it replaces old login pages of electronic services. Instead of authenticating users by themselves, when necessary, the services redirect the user to MPass, which in turn asks users to authenticate with any number of convenient authentication devices (e.g., mobile phone, national electronic ID card, government employee card or USB token) using qualified certificates and entering the correct PIN code. In case of successful user authentication, MPass issues an authentication ticket signed by itself and sends it back to the calling service. The authentication ticket is a proof of successful user authentication and may contain additional user-related claims used in authorization. Thus, MPass abstracts e-services from the complexity of dealing with multiple devices, authorities, and technical interfaces. It offers reliable single sign-on and single sign-out, thus contributing to better security and enhanced user experience. For the end user, the authentication sequence is simple and involves a few steps: (i) user accesses the e-service;

(ii) e-service redirects the user to MPass authentication page, where the list of available authentication devices is displayed; (iii) depending on the chosen device, the user inputs phone number (only if Mobile eID was chosen) and PIN; and (iv) in case of successful authentication, the user is redirected back to e-service.

MPass architecture, presented in Figure 7 below, is based on the provider architectural pattern, where different authentication methods and devices are implemented as separate modules, called *identity providers,* which are integrated into the MPass core using a unified technical interface. This allows new authentication methods to be added without affecting the entire service or the e-services that use MPass. For instance, if at a certain time it is decided that a biometric authentication option should be made available, a new authentication module can be developed and integrated into MPass core. This would then instantly make biometric authentication available across all integrated e-services with no effort on the e-service providers' side.

Figure 7. MPass Architecture



MPass relies on open standards for authentication and authorization and uses claims-based security[20] with an SAML 2.0 protocol. This contributes to a high technical compliance with other information systems and greater sustainability.

20 Claims represent additional authorization data from various sources that allow fine-grained access to various information systems and/or functions within an information system (for example granting a user access to a government IT system based on information from a registry of public servants that he is an active government employee).

The MPass authentication service not only minimizes technical complexities related to electronic identity for e-service providers, but it also offers contractual independence for various signature service providers. Sectorial e-service providers are not forced to sign bilateral contracts with all signature service providers, instead, they sign one single agreement with the e-Governance Agency, the owner of MPass, and the agency take care of the rest.

The government regulates the use of MPass, as any other governmental service. The government Decision No. 1090 regulating MPass[21] makes this service mandatory to be used by central public authorities and recommends it for local governments and private sector.

For public authorities, the use of MPass is free of charge and subject to signing of an agreement with the eGovernance Agency (EGA). Private companies are charged a small transaction fee for each authentication upon signing a contract with EGA. The integration is first done on a test environment, and transition to production is done when case integration tests are successfully run.

MSign—digital signing and signature validation service

MSign—the government electronic signature service—is technically and contractually very similar to MPass. MSign is a centralized service which provides digital signature and signature validation functionalities to integrated services. When a service needs a signed document or transaction, it asks MSign to produce the signature by passing data to be signed and the control to it. MSign in turn asks the user what device with qualified certificate will be used for signing and instructs the user to apply the electronic signature with that device. In case of successful signing, the signature is passed back to the calling service for further processing. Later, if a service that keeps signed documents needs to validate early applied signatures, it passes them to MSign for signature validation and receives the result. Multiple signing scenarios, like basic signing, cosigning, and countersigning are available.

As in the case of MPass, MSign frees e-service providers from the complexity of dealing with multiple devices, authorities, and technical interfaces.

MSign architecture (Figure 8) is also based on the provider architectural pattern, where different signing methods and devices are implemented as separate modules—signature providers—integrated into the MSign core using a unified technical interface allowing new signature methods to be added without affecting the entire service. For instance, if at certain time hardware security modules (HSMs) would be needed for server-side signing, then once integrated into MSign core, the new signing provider will instantly make server-side signing available for all integrated e-services, with no effort on the e-service providers side while offering new opportunities for end users such as mass document signing, etc.

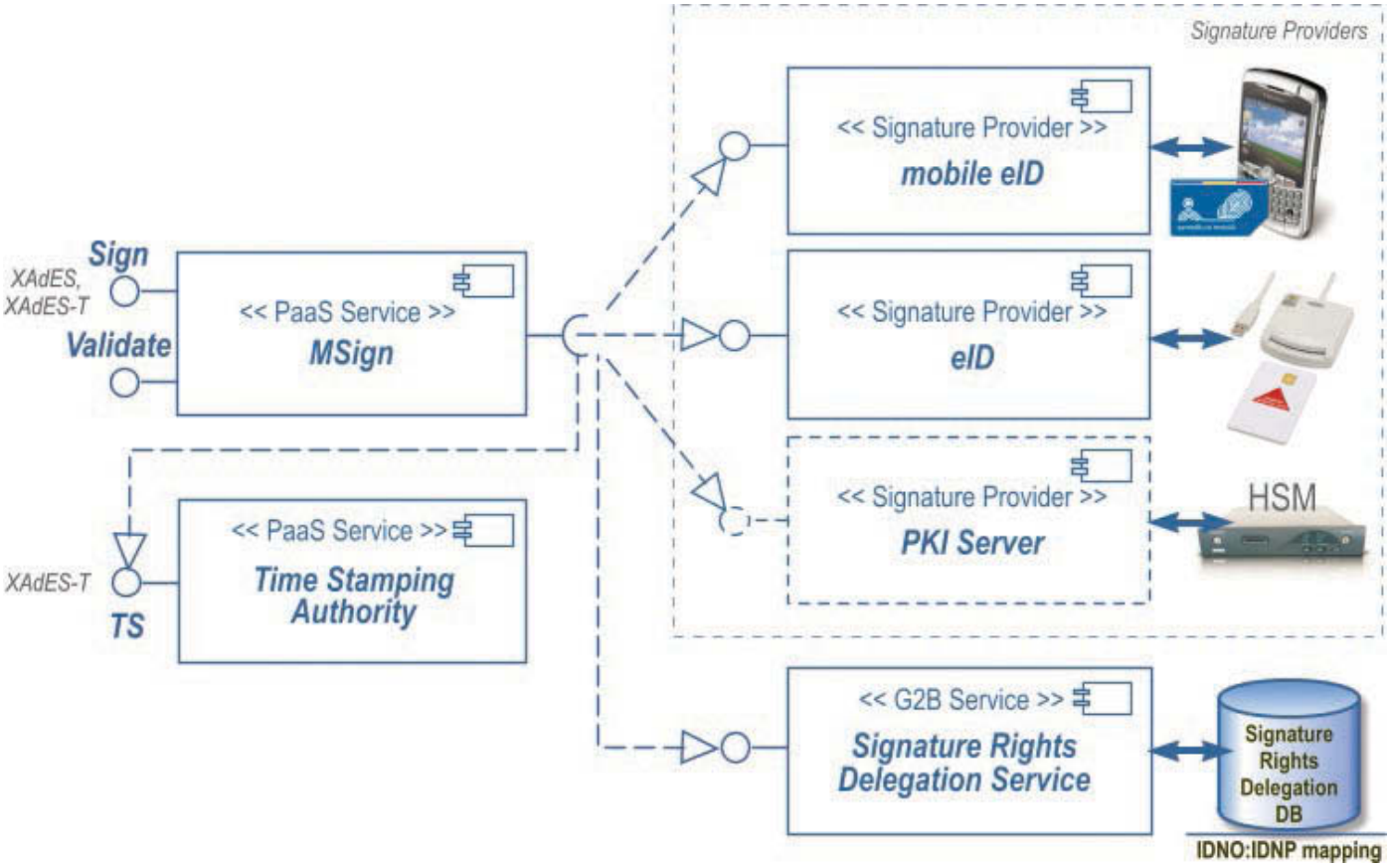
Similar to MPass, MSign relies on open standards for digital signatures, working with XAdES and PAdES signature formats. This contributes to a high technical compliance with other information systems and better sustainability of the digital signing infrastructure.

The e-Governance Agency delivers MSign using the same model as in MPass, offering contractual independence on various signature service providers. Sectorial e-service providers are not forced to sign bilateral contracts with all signature service providers, instead, they sign one agreement with the eGovernance Agency.

The use of MSign is regulated by the government Decision No. 405,[22] which makes this service mandatory to central public authorities who require legally binding e-signatures for transaction completion (e.g.,

21 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=351035&lang=2
22 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353239&lang=2

Figure 8. MSign Architecture



provision of a public service, submission of an e-report, declaration, etc.) and recommends it for local governments and the private sector.

MPower—authorization registry

For a while, it was a common practice for certification authorities in Moldova to issue two types of digital certificates to their customers—for individuals and for legal entity representatives. The certificates issued to legal entity representatives had all the attributes contained in a certificate issued for individual persons plus it had the IDNO of the legal entity and the position the individual held in that organization. When accepting documents signed with such certificates, authorities have to make sure that all business rules are strictly followed. For instance, if an invoice needs the signature of the accountant of a particular entity, then the appropriate certificate attributes have to be considered.

The reality is that people are quite often migrating from one position to another within the same organization or between organizations. In this case, the certificate issued to a person as a representative of a legal entity with hardcoded IDNO and position within the organization must be revoked, and a new certificate with new attributes has to be issued. The timely revocation of old certificates is the responsibility of the administrator of the organization owning the certificate. In absence of a consistent and reliable certificate management and prompt certification revocation mechanism, this situation weakens organization security since revocation may take from several hours to several days. The subject of the still valid certificate can abusively access electronic services and resources which they are not supposed to access anymore. To mitigate these risks, many authorities decided to do additional checks against the information they collect

internally instead of certificate attributes. Although this does not fully solve the problem, it does reduce some risks of abuse.

The actual solution of the problem is the registry of authorizations called **MPower,** which is currently being implemented by e-Governance Agencies and which facilitates mapping of different individuals to legal entities based on declarations signed by the administrators of the legal entity, thus empowering individuals (giving them power of attorney) to act on behalf of legal entities. For example, if an administrator of an organization nominates someone as chief accountant, the administrator can access MPower and create a declaration where the personal identification number of the chief accountant is mapped to the organization with particular IDNO in the role of "chief accountant." The declaration is signed by the administrator using MSign and registered into MPower. From that point on, whoever needs to accept transactions from the chief accountant of that organization will deal with the designated person as per signed declaration in MPower. That is, the Tax Authority or Social Assistance Authority, for instance, will rely solely on information from MPower without collecting the same information from legal entities multiple times.

When an authorized person resigns or is transferred to another position, the administrator creates and signs corresponding declarations in MPower. As a result, all previously assigned authorizations are instantly revoked.

Although the MPower concept was created to replace digital certificates issued for legal entity representatives, it may be used to accommodate other interaction scenarios like individual-to-individual or organization-to-organization authorizations (i.e., MPower acts as a repository of electronic powers of attorney for individuals and businesses) revealing great potential for remotely accessible services and for use of digital signatures.

7. Lessons Learned

There are a few valuable lessons learned that can apply to other countries that consider embarking on implementation of Mobile eID. These fall under a few areas, such as:

1. **Generating and maintaining political support**
   - **Exploit the visibility and publicity** that the government will benefit by being one of the very few countries in the world to implement a mobile eID;
   - **Highlight the transformative potential for mobile eID,** such as eliminating queues at service points and reducing potential for bribery in G2C and G2B interactions;
   - **Plan for incremental steps and capitalize on early success.** Balance visible activities with complex under-the-hood implementations; and
   - If the country has many citizens who live abroad, better serve their needs through the mobile eID part of the political agenda.
2. **Generating and maintaining interest of public and private partners**
   - **Ensure that an enabling environment is present,** adjust it as appropriate, and avoid potential pitfalls (e.g., cumbersome laws on PPP, etc.);
   - **Stimulate competition to increase development and improve uptake and accessibility of electronic signatures for citizens and businesses.** With the implementation of mobile signature, the rest of the providers rapidly improved their own infrastructures, making their electronic signature token compatible with a broader range of devices and operating systems, while reducing the cost of this technology for the end user;
   - **Leverage MNOs' capacity to reach a critical mass of the population** with an eID. Due to their experience with Know-Your-Customer (KYC) procedures, they are likely to be able to provide registration services with relative ease and verify their customers' ID at the point of registration (provided all the components, like a robust foundational ID system/population registry, PKI, etc., are in place);
   - **Promote inclusivity, nondiscrimination, and equal rights for all participants.** Ensuring that customers of all electronic signature providers can use the signatures for all e-services indiscriminately offers providers additional space for development and growth and added convenience for end users;
   - **Give negotiation processes sufficient time and attention.** It often takes time to raise the interest and gain the trust of certain partners; do not rush decisions and allow all parties to give design and implementation options careful thought; and
   - **Ensure sufficient capacity on the side of the public partner** by bringing the best talent to manage the process. The Moldovan government realized that in order to bring in a strong technical team, there was a need to offer competitive salaries. Therefore, the staff of the eGovernment center was selected on a competitive basis and comes from the top IT companies.
3. **Thoroughly planning solution architecture and technical aspects**
   - **Avoid duplication and stimulate reuse of common functionalities.** Until the implementation of shared government services for authentication (MPass) and electronic signature (MSign), each service and eID provider was developing their own modules for authentication and electronic signing of documents and records. These individual modules were both expensive to develop and maintain, as well as technologically difficult for end users to handle. With the rollout of MPass and MSign, GoM has seen a surge in the number of eservices that uses electronic signatures for

robust remote authentication. MPass and MSign provide abstraction layers both for end users and e-service providers. This provides end users with a familiar interface irrespective of the e-service or IT system they use. E-service providers are also spared the necessity to update their systems every time there are changes in the middleware of the eID providers (e.g., the switch from Java applets to alternative solutions due to browser limitations was done without affecting any of the 40+ systems integrating MSign).

- **Allow for one signature for both individuals and legal entities.** To make life easier for the end-users of electronic signatures, Moldova is allowing the use of the same private key certificate for electronically signing transactions in both Government to Citizen (G2C) and Government to Business (G2B) scenarios, which means that users do not need multiple certificates (though they can get as many as they want) in order to interact electronically with the government.
- **Use open standards to ensure interoperability and sustainability.** Having a clear set of international and open standards was a key success factor that allowed for seamless integration of all eID providers in the government's shared infrastructure and makes administration of PKI more cost efficient.
- **Use open APIs for seamless integration with 3rd party systems.** The fact that MPass and MSign offered open APIs for integration with other systems led to the fact that not only government agencies are integrating them, but also the private sector is increasingly interested in reusing the shared authentication an electronic signature infrastructure.

It was not until MeID was integrated in MPass and later in MSign that the Mobile ID gained real traction, becoming a universal tool for authentication into government systems and for e-service delivery. So it's important to introduce mobile ID alongside other tools.

Annex 1. Applicable Laws and Technical Standards

The technical standards regarding advanced qualified electronic signatures are approved by **Order of the Security and Intelligence Service No. 69 of 15.07.2016** regarding the approval of technical norms in the field of advanced qualified electronic signatures.[23]

The private and public keys used to create a qualified advanced electronic signature are created by the provider through the secure signature creation device in accordance with **FIPS 140-2 Security Requirements for Cryptographic Modules, Level 3 or 4;** or **SMV CWA 14169: 2008 "EAL4 +" Signature Safety Devices,** or **SM ISO/CEI 19790: 2012 Information Technology–Security Techniques–Security Requirements for Cryptographic Modules.**

The management of public and private keys is performed in accordance with the **IETF RFC 6712 Internet Protocol X.509 Public Key Infrastructure (HTTP) Transfer Protocol (CMP) protocol, IETF RFC 4211 CRMF).** The secure signature device containing the advanced qualified private key, must, in addition, meet the requirements of the **PKCS # 15 Cryptographic Token Information Format Standard.**

The advanced qualified signature format must meet the requirements of **PKCS # 7 Cryptographic Message Syntax Standard** and/or **Advanced XML Signatures (XAdES)** and/or **Advanced PDF Signature (PAdES),** and the providers must use the **SHA-256** hash function.

According to the legislation, the **minimum length of public and private keys is 2048 bits** for the RSA algorithm for qualified advanced electronic signatures users and 4096 bits for the RSA algorithm for providers. The validity of the public key certificates of the higher level certification service provider is 20 years, that of the public key certificate of the level two certification service provider is 10 years, and the validity period of the public key certificate of the users cannot exceed five years, depending on the capabilities of the secure signature creation device, which mainly is dictating the length of keys. For keys with a length of 2048 bits the validity period is two years, for 3072 bits three years and for 4096 bits five years. The validity period of the private key of the Time Stamping Service (TSP), Online Certificate Status Protocol (OCSP), Data Validation and Certification Server (DVCS) five years.

23 http://lex.justice.md/ru/365884/. The full list of all applicable standards can be found at the following link http://pki.sis.md/standardele_pki.

Annex 2. Evolution of Moldova Public Key Infrastructure

The public key infrastructure in Moldova was established in September 2005, following the approval of the law on digital signatures and electronic documents in July 2004.[24] The government approved the regulations on the functioning of certification authorities and appointed the Security and Intelligence Service (SIS) as the root certification authority. In the next 12 months, SIS approved technical regulations on devices and other technical means accepted for qualified digital signature business.

In September 2006, the Center for Special Telecommunications (CSTs) launched the first intermediate certification authority providing digital signature services, including qualified signatures for government, businesses, and citizens. CST started with the CryptoCertum 3.0 cryptographic smart card as a secure signature creation device for advanced qualified signatures. The cost of an electronic signature kit, including the smart card, card reader, keys, and certified public key was about 100 USD—a price that was much too high for the limited applicability it offered. Hence, the number of active qualified certificates issued to individual persons until September 2012 did not exceed 50 certificates. Another inconvenience for obtaining a digital signature kit was the fact that these services were provided from one single location for the whole country. The main beneficiaries of certification services at the time were private entities, especially commercial banks, which were using signatures in their interbanking message exchange. This situation did not favor in any way government aspirations to implement its digital development agenda, especially to digitize all public services and let citizens and businesses access them remotely using strong authentication and electronic signing of the digital content.

In September 2008, the state-owned enterprise FiscServInform (FSI) was created, and in April 2009, it was appointed as the main technology provider to the Tax Authority. One of the first priorities for FiscServInform was to let individuals and legal entities submit their tax declarations and reports electronically. Considering the high price for the qualified digital certification services, the Tax Authority decided to issue unqualified digital certificates for taxpayers, thus limiting the applicability of the qualified signatures only to tax services on the one hand and making digital signing a common and affordable practice in the business community on the other hand.

The Tax Authority, through FiscServInform, established an internal certification authority providing unqualified certification services and not following all the rigors of a qualified signature provider. It created three service delivery points—registration authorities—issuing unqualified certificates free of charge on unprotected CDROMs. Though these certificates did not correspond to the technical requirements of the central certification authority, signing bilateral contracts with taxpayers provided the legal force of such electronic signatures. During the period of 2006–2012, approximately 170,000 signatures were issued. Starting on January 1, 2012, all VAT paying companies were forced to electronically sign and submit tax declarations, which increased the popularity of the certificates issued by FiscServInform, even though qualified certificates issued by CST for authentication and signing were also accepted. Starting with March 2016, FiscServInform ceased issuing unqualified certificates, as it became an accredited Certification Authority and started issuing advanced qualified electronic signatures. In October 2017, the last advanced unqualified certificates issued by FSI expired.

Considering digital development, some other state authorities, such as the National Chamber for Social Insurance, the National Bureau of Statistics, and others, were inclined to adopt electronic submission

24 http://lex.justice.md/ru/313061/

of reports from businesses. However, establishing their own certification authority issuing unqualified certificates as per the Tax Authority model, with all the hassle related to bilateral contracts, was not an option for these organizations because the price for qualified signature services still was too high.

In order to solve the affordability problem of qualified digital signatures, the government launched the Mobile eID on September 14, 2012, which immediately lowered the price of alternative eID devices.

In May 2014, the government started to issue its first electronic identification cards with contactless interface. The issuing authority, state-owned enterprise *Registru*, set up its own certification authority providing qualified signature services. Since eID cards were being issued along with simple plastic non-electronic ID cards, due to high prices for electronic ID cards, their uptake was quite insignificant.

In May 2018, as part of a larger public-sector IT reform, the government consolidated all state-owned signature service providers into a single certification authority, operated by public institution *ITSec Service* (former SOE *Center for Special Telecommunications*) with multiple registration authorities such as the newly established *Agency for Public Services* (based on former SOE *Registru*), Tax Authority offices, and mobile network operators.

Annex 3. Technical Specifications of Available Electronic Signature Devices

CryptoCertum 3.0 smart card

The CryptoCertum 3.0 cryptographic card was first introduced in 2006 and was the first secure signature device available to Moldovan citizens. Some of the card's key features include:

- Manages RSA 2048 bits cryptographic keys
- Performs SHA-256 hash function
- Supports DES, 3DES algorithms
- Secures computer access: removing the card from the reader blocks access to the computer, inserting it into the reader, and entering the PIN code unlocks access to the computer

CryptoCertum cards are also used as a basis for personalized access cards for government employees. Such cards help identify government employees and allow access to government facilities. They also allow the employee to be identified within the Civil Service Electronic Identification System and electronically sign documents and records.

USB tokens

CryptoMate64 is a device for authentication and storage of the public key certificate and digital signatures, which combines the security of certificate-based technology with the simplicity of plug-and-play usage. It was first introduced in 2011 and has the following features:

- High-performance smart card chip
- Incorporates 1024-bit and 2048-bit RSA key generation
- Algorithms incorporated: RSA, AES, DES / 3DES, SHA-1, SHA-256
- Authentication and signature digital signature for PKCS # 11

ePass 2003 Auto is a fully plug and play cryptographic device for digital identity verification, which allows for protection measures for communications and digital transactions. ePass2003 can provide desktop and network logging both locally and remotely. Cryptographic keys and digital signing of e-mails, documents, and transactions are made onboard in a safe environment that prevents change and manipulation. Other features include:

- High-performance smart card chip
- Incorporates 1024-bit and 2048-bit RSA key generation
- Algorithms incorporated: RSA, AES, DES / 3DES, SHA-1, SHA-256
- Random Number Hardware Generator

Mobile eID

The Mobile eID is using a client-side model, whereby the private key is stored on a special crypto processor–enabled SIM card. The Gemalto UICC-based technology was chosen by the mobile network operators due to its compatibility with all types of mobile telephones used in Moldova (both smartphones and older handsets). The technology allows citizens to confirm their identity and sign documents directly from their mobile phone, by entering a unique user-selected PIN code. The embedded Valimo Mobile eID application transforms any mobile handset into a device capable of delivering strong user authentication and legally binding signatures, which are essential for securing e-government services and transactions.

Electronic ID card

The third generation electronic ID cards are produced on an ID-I format, made of polycarbonate and are fully ICAO-compliant. eIDs are built on a modern contactless NFC interface in full compliance with *ISO/IEC 14443 Identification cards—Contactless integrated circuit cards—Proximity cards* standard.

Annex 4. Differences between Client-side and Server-side MeID Models

Client-side mobile identification

One approach for implementing mobile electronic identification is to perform digital signatures directly on the phone, using built-in secure elements on special SIM cards or secure elements implemented on an external hardware plugged into the handset.

In this case, the private key needed to conduct signatures is stored within these secure elements. Its usage is protected by a PIN known only to the holder of the phone so that the holder has the exclusive control over her/his credentials. The result of a digital signature is usually transferred to a communication partner, either using a GSM channel or some other communication technology like RFID, NFC, or Bluetooth.

An already approved solution is the integration of a PKI module within a Subscriber Identity Module (SIM). This approach seems obvious since SIM cards are already installed and integrated in the phone, the distribution is ensured by the mobile operator, and private keys can be generated on-card, so that they never leave the secure environment.

A SIM is a module that securely stores network specific information used to identify and authenticate subscribers on the network, e.g.:

- Like every smart card, a SIM provides a so called “Integrated Circuit Card ID” (ICCID), an international unique identifier;
- The International Mobile Subscriber Identity (IMSI), a unique identifier used by individual operator networks; and
- An authentication key used to authenticate the SIM on the mobile network.

Each subscriber is uniquely linked to the SIM, which stores the user's private key needed for authentication based on signatures in a tamperproof manner. A SIM card in a phone can be regarded as a smart card fully integrated with reader and display in combination with networking functions.

The processes of registration, authentication, or signing may differ from case to case, as outlined below:

User registration process

1. The user gets a WPKI capable SIM card from the mobile operator.
2. If there are already private keys stored on the card, the PKCS # 10 files and the public device certificates are already stored at the mobile operator.
3. The registration/certification authority (RA/CA) verifies the user's identity (not in scope of WPKI) and sends an activation code to the user.
4. The user contacts the RA/CA to start the activation process. Depending on the phone number, the RA/CA identifies the appropriate mobile operator.
5. The RA/CA contacts the mobile operator via WPKI interface in order to start the activation process. The mobile operator checks if the user's SIM card already has pre-distributed keys included. If not, a

special command is sent to the user's SIM card in order to start an on-board key generation process which involves the definition of the PIN codes.

6. The RA/CA receives the device certificate.
7. The RA/CA sends a signature request through the mobile operator to the user's SIM card.
8. The user is asked to enter the activation code which he additionally has to sign using his PIN code.
9. The signed code is returned to the RA/CA through the mobile operator.
10. The RA/CA verifies the signature and the activation code.
11. The RA/CA receives the PKCS # 10 requests from the mobile operator.
12. The RA/CA generates the user certificates.
13. The user is informed upon the successful activation process.

Authentication process

1. The user wants to authenticate against a relying party. The relying party asks him for his phone number. The user enters his phone number.
2. The relying party performs a lookup by contacting each trusted registration/certification authority (RA/CA) via the WPKI search interface. If there are multiple search results (the user may be registered at several RA/CAs) for a given phone number, the user has to choose a RA/CA.
3. The relying party displays the information to be signed on the "information channel" (the user's browser for instance) including the instruction that the user should sign using the security channel (his cell phone). An optional control code may also be displayed.
4. The user's SIM card receives a signature request.
5. If a control code was used, the user has to enter the particular control code on the mobile phone. The user signs the displayed text by entering the PIN.
6. The mobile operator sends the signed message to the relying party, which performs signature verification as well as a certificate validation sending an OCSP request to the RA/CA.
7. The RA/CA returns the certificate status.

Signing process

1. The user wants to use a service that needs authentication.
2. The user enters the number of his cell phone into the web form of the service he wants to authenticate against.
3. The cell phone receives an especially prepared SMS message from the service provider containing the text to be signed.
4. The user counterchecks the message text.
5. The user signs the message by entering his 4-digit PIN.
6. The message is signed using the SIM's PKCS # 1 functionality.
7. The signed message is sent back together with the SIM's unique ICCID.
8. The verifying authority checks the signature. The certificate containing the public key needed to verify the signature may be retrieved by means of the ICCID transmitted by the signer.
9. The user is now authenticated upon the service provider.

Server-side mobile identification

This innovative approach, which was presented to the public in the framework of the E-Government Ministerial Conference in Malmö at the end of 2009, enables qualified electronic signatures without additional software installation and hardware such as smart card readers.

In contrast to client-side Mobile eID solutions, the server-side mobile phone signature is not based on specific SIM cards, as the signature-creation data is stored remotely. Thus, it is not the mobile phone itself holding the secure signature creation device required for qualified electronic signatures but a remote hardware security module. In the server-side model, any mobile phone on any mobile operator network can be used, as it does not require a specific SIM card and therefore does not require the user to change the previous SIM card. The only technical requirement is for the mobile phone to be able to send and receive an SMS.

Similar to many solutions used by banks for e-banking purposes, after typing the phone number (as user ID) and password, the user receives an SMS to the registered mobile phone containing a one-time ephemeral code (TAN). Entering this TAN, a qualified electronic signature is triggered using a qualified certificate and signature creation data stored in a HSM securely held by the provider.

User registration process

The technical process for the generation of signature creation data is performed in the HSM in the course of the initial registration process:

1. The identity of the signatory is verified by the certification service provider in accordance with the legal requirements. During the registration process, the signatory has to define the mobile phone number that he/she wants to use to trigger the signature process in the future and chooses a secret password.
2. The actual possession of the specified mobile phone number is verified by immediately sending an SMS to that device containing an ephemeral one-time code (transaction number TAN).
3. The signatory has to enter the TAN into a web form.
4. After verification of the TAN by the service, the new signature creation data are generated in the HSM, and the generated private key is immediately encrypted again with another key that is derived from the mobile phone number and the password of the user. Through this, the encrypted private key is only usable later on if the secret password is available for decryption. To also ensure that the usage of the private key is only possible inside the certified HSM, the encrypted private key is encrypted again—this time with a key known only to the HSM. This double-encrypted signature creation data can be stored even outside of the certified HSM in a key database.

Authentication process

A typical process of authentication may be conducted as follows:

1. A user wants to authenticate against a service provider.
2. The service provider redirects the user to the authentication authority.
3. The user enters his phone number and a password. The password is needed in order to prevent misuse of the service.
4. The authentication authority transmits a TAN valid only for a short time period optionally together with a hash value of the authentication message to be signed to the clients' phone via an SMS.
5. The user checks the authentication message he is going to sign online and compares its hash value with the value he has just received.

6. If the values match, the user enters the TAN together with the PIN related to his private key in a web form.
7. The server signs the authentication message using the HSM and the PIN code provided.
8. The result of this signature is sent to the service provider.
9. The service provider performs a signature verification as well as a certificate validation.
10. Upon successful verification, the service provider accepts the user's authentication.

The signing process

The subsequent use of the signature creation data for signature creation is similar to the described registration process:

1. If a user wants to sign a document, he/she triggers a signature request of the application in use (be it a web application or locally installed software). This signature request includes the documents/ data to be signed and is directed toward the provider of the mobile phone signature.
2. As soon as the request is received by the HSM, the user has to enter his/her mobile phone number (which serves as the User-ID) and his secret password. All these entries are processed through secure communication channels directly in the web application of the mobile phone signature.
3. After examining whether the specified number matches the registered signatory, the document/ data to be signed, including the password and phone number, are immediately passed to the HSM. The HSM subsequently calculates a hash value ('digital fingerprint') of the document/data and a random ephemeral one-time code. Both are sent by SMS to the specified mobile phone. In parallel, the signatory is offered by the web application of the mobile phone signature service to see and check once again the data to be signed. At the same time, the short hash value is displayed by the web application.
4. The signatory receives the SMS and has the opportunity to compare the hash value received by SMS with the hash value displayed by the web application. By entering the received TAN into the web front-end of the mobile phone signature service, it is assured that the signatory is actually in possession of the registered mobile phone.
5. This positive verification causes the HSM to retrieve the associated encrypted signature creation data from the key database and to decrypt it with the secret key of the HSM. In the next step, this—still encrypted—signature creation data is decrypted using the derivation of the secret password of the user. Only now the private key is available in the certified HSM.
6. The signature is created in the HSM and the signed document/data is handed over to the signatory.

Both the decryption of the signature creation data and the creation of the signature itself are performed exclusively within the certified HSM, and the selected decryption mechanisms assure that this is technically possible only there. From this perspective, the security of the created signature is equal to that of a smart card–based solution. Also, from the perspective of the signatory, the process is comparable—the signature process is triggered with two components: disclosure of the secret password (factor "knowledge") and mobile phone number and positive verification of the possession of the mobile phone (factor "possession"). The "knowledge" factor is verified by the HSM itself in the process of decryption of the signature creation data. The verification of the "possession" factor is carried out by the secure signature application, which also includes the connection to the peripheral elements, such as SMS gateway or web front-end.

id4d.worldbank.org