REGIONAL INITIATIVES – EUROPE

MOBILE IDENTIFICATION: IMPLEMENTATION, CHALLENGES AND OPPORTUNITIES

Telecommunication Development Sector

Mobile identification: Implementation, challenges, and opportunities

This compilation of national implementations of Mobile ID (m-ID) was prepared by the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU), in collaboration with the Ministry of Digital Affairs of the Republic of Poland. This report would not have been realized without the input provided by the experts who attended the ITU Mobile ID (m-ID) Expert Group Meeting on 18-19 October 2016, within the framework of the ITU Regional Initiative for Europe on Innovation, and in partnership with the Office for Electronic Communications of the Republic of Poland, which brought together experts from Austria, Azerbaijan, Estonia, Latvia, Malaysia, Oman, Poland, Spain and GSMA.

ISBN:

978-92-61-24601-3 (paper version)

978-92-61-24611-2 (electronic version)

978-92-61-24621-1 (EPUB version)

978-92-61-24631-0 (Mobi version)

Please consider the environment before printing this report.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

List of tables, figures and boxes

Figures

1 Background and purpose

To optimise the use of the ICT infrastructure at national and global levels, governments have embraced services that allow their citizens to electronically access services (e-services) from public and private organisations using a secure citizen identification in the virtual world – the electronic ID (e-ID).

The explosion in the uptake of wireless and mobile technology is increasingly affecting how public institutions function and deliver services. In 2016, the number of mobile subscribers worldwide reached over 7 million whilst the cellular-mobile penetration rate stood at 99.7 worldwide, 126.7 for developed countries and 94.1 developing countries. The use of a citizen identification tied to the citizen's mobile phone – mobile ID or m-ID- has been a natural evolution from e-ID for some countries whilst in other countries, it is considered as a way to leapfrog from paper to mobile electronic services (m-services). M-Government – mobile government- provides services to a wide user base and at the same time lends itself to the deployment of m-services that could not have been conceptualised on the pure e-platform.

The adoption of the m-Government model to support and enhance government performance and a more connected society is inevitable. M-Government emerges as the next generation in the process of information and communication technology (ICT) use in the public sector. Mobile access to government services allows developing countries to bypass building the heavy (fixed) network infrastructure, which reduces costs and time.

Sharing of implementation experiences on Mobile ID at an international level and addressing challenges collectively is paramount to enhancing future deployments and rectifying existing roll-outs. It is in this spirit that the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU), in collaboration with the Ministry of Digital Affairs of the Republic of Poland, organized a Mobile ID (m-ID) Expert Group Meeting on 18-19 October 2016, within the framework of the ITU Regional Initiative for Europe on Innovation adopted by the World Telecommunication Development Conference (WTDC-14). The aim of the expert group meeting was to present ideas about innovative mobile identity solutions and share experience about past and current implementation efforts based on an initial set of questions (annex A).

This report sets out practical proposals that will further the discussions and information sharing on the issues surrounding m-ID, and includes a compilation of the contributions received as part of the expert group meeting (annex B).

2 Approach

Using the presentations made at the expert meeting as a basis, countries and organization representatives were requested to submit examples of their m-ID experience. These examples have been reproduced in annex B. Elements from these contributions as well as work undertaken by ITU that are of relevance to m-ID is elaborated in section 3. A set of proposals is provided for future consideration in section 4.

3 Current situation

Mobile ID is essentially a secure authentication system for citizens to access m-services or e-services. Location is a differentiating factor between e-ID and m-ID. Location provides opportunities for location based m-services but it may also introduce privacy concerns. Based on the contributions received from the experts and reproduced in annex B, some enabling elements for rolling out m-ID, and associated challenges, were identified, including:

Mobile ID enablers

- A wide mobile user base in the country facilitates standard as well as customised e-service deployment.
- Mobile connectivity is reliable, affordable and has a wide coverage.
- E-services (from government as well as the private sector) are accepted and requested by citizens.
- There is a push for m-ID roll-out from the private sector.
- A few e-services that have a direct socio-economic impact have been identified and will be deployed as 'quick wins' when m-ID is launched.
- The legislative environment is favourable to m-ID implementation.
- The security component of m-ID is handled in the most effective way for upholding confidentiality, integrity and availability of information.

Mobile ID challenges

- Selection of the appropriate, stable, and scalable technical solution given the rapid advances in ICTs can reduce the risk of the solution being made obsolete within a few years.
- Interoperability of the solution within regional groups and other partner countries.
- Acceptance by the private sector to use the m-ID solution to deploy their services.
- Acceptance of users who may have alternative ways of making transactions, which they perceive as more efficient and reliable.
- Public trust in electronic transactions and in data protection by public entities.

Securing identification of citizens and e-transactions is often achieved through a public key infrastructure (PKI). This uses a dual authentication system in which a digital signature, created through a complex random algorithm using a private key on the card, is checked up against a public key on a database. ITU-T Recommendation X.1122[1] serves as a guideline for implementing PKI security in mobile systems.

The ITU Telecommunication Development Bureau (BDT) undertakes several actions to spread equitable and affordable access to ICTs as a means of stimulating broader social and economic development. One of the areas of action is ICT applications: e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of Sustainable Development Goals (especially SDGs 1, 4, 6, 7, 13, 14, 15, 17). Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may liberate technical and human capacity and enable greater access to basic services.

M-Government: Mobile Technologies for Responsive Governments and Connected Societies[2] a 2011 joint report of the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD) and the United Nations Department of Economic and Social Affairs (UNDESA), documents the use of mobile technologies to enhance government performance, improve public service delivery, and engage citizens and civil society organizations in policy and

[1] https://www.itu.int/rec/T-REC-X.1122-200404-I/en

[2] www.itu.int/pub/D-STR-GOV.M_GOV-2011

decision making both in developed and developing countries. This report provides elements for consideration for not only a successful deployment of m-ID but a successful roll-out of mobile services that makes a difference to the lives of citizens and has an impact at the socio-economic level. The report has specific chapters dedicated to the benefits and outcomes of m-government, understanding m-government adoption, and technology options for mobile solutions.

Figure 1: mGovernment value chain

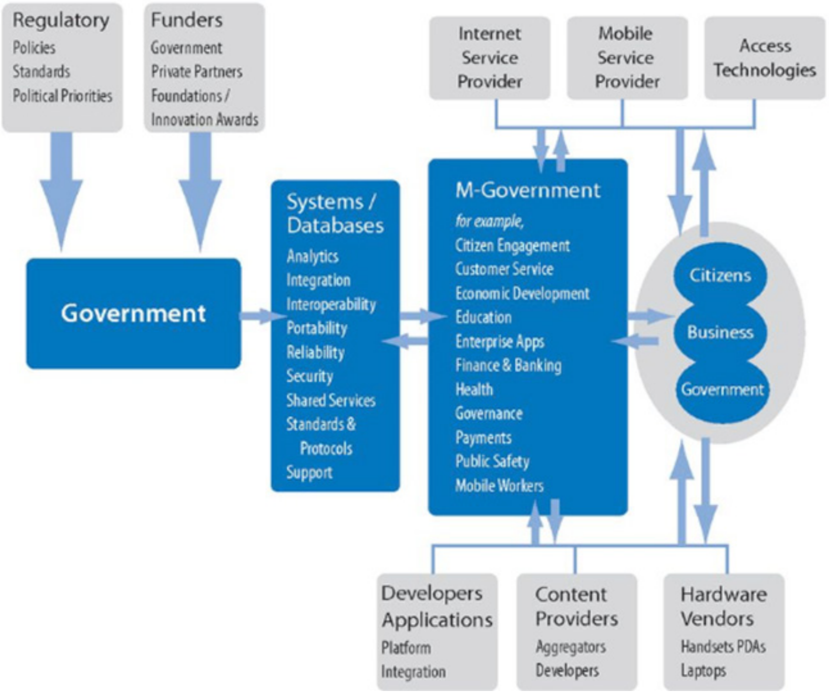
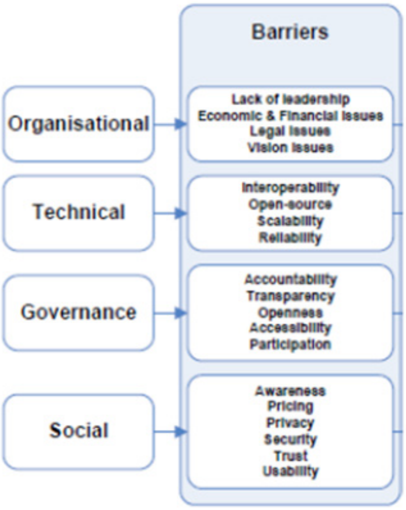


Figure 2: Barriers to mGovernment



There are some challenges to the implementation of mobile government service:

- The existence of m-Government and its applications does not on its own guarantee results and governments should proactively consult with the public and take their opinion into account before implementation.

- Users expect transparency, a free flow of information about government decisions and actions. Transparency is part of, and cannot be separated from, accountability; risks will arise when one of them is applied and the other is neglected.
- If a delivery process is not effective and needs to be re-organized, it might cost even more correcting it than later putting it on the mobile delivery channel.
- Creating a uniform user interface for services and multi-jurisdictional service delivery.
- Ensuring technology portability from older systems to m-Government interfaces.

The 2011 M-Government report also provides a checklist that can be used as a preliminary guide to orient governments from a policy/strategy perspective is and has valuable elements for future consideration. A broader all-encompassing approach going beyond m-ID towards mobile services for achieving Sustainable Development Goals, will be needed for a total engagement of all stakeholders and a successful roll-out with all perspectives carefully factored in.

4 Way forward

Implications from diverse perspectives namely policy, strategy, legislation, technology (connectivity, security, scalability), stakeholders (awareness, engagement), services (identification, deployment, user group build up) need to be researched and assessed. The case for deploying m-ID needs to have a cost benefit analysis, a review of approaches to deployment (government only, public-private partnerships, bilateral assistance) and of service provisioning methods (government, private sector, citizen customisation).

The burgeoning platform for information sharing in the Europe region may be strengthened and extended to a global platform. A few proposals for future consideration for furthering the dialogue on m-ID are listed below. Should there be, for any proposal, a similar existing initiative, collaboration with that initiative should be considered for optimal resource use.

1. Maintain an up-to-date list with details of focal points, websites, and summary texts:
   a) of countries having implemented, currently implementing or planning a roll-out of m-ID in Europe and globally;
   b) of international and regional organisations active in the m-ID arena;
   c) of organisations with proven experience in rolling out m-ID at the national level;
   d) of countries willing to share their successfully m-ID implementation experience and know-how with others;
   e) of organisations with proven experience in providing training in m-ID;
   f) of m-ID capacity building events.
2. Develop awareness material for governments to understand the cost-benefits of m-ID deployment as well as the challenges to be handled, backed by concrete examples.
3. Elaborate a set of guidelines for countries to consult and act on, prior to engaging m-ID roll-out.

5 Conclusion

Mobile ID provides a number of benefits: it is more convenient for users, and it is cost effective (for deploying agencies) when leveraging the digital transformation. Aspects to be given due consideration during deployment of m-ID include ID management and user enrolment; the issuance and life-cycle-management of credentials; the usage and storage of credentials; and ultimately the uses of m-ID for authentication, authorization, encryption, and signatures in a number of different scenarios. Some of the interoperability, security, and scalability challenges associated with the deployment and management of m-ID are being solved by a number of standards and technologies.

According to the Security Identity Alliance[3], it is anticipated that digital transformation saves governments worldwide up to USD 50 billion annually by 2020. The critical mass of digital natives that will foster mobile services at national seems to have been reached on a regional and global level. Mobile ID is one link in the chain to connect the unconnected and thus connect the world through ubiquitous services beyond e-Government and m-Government where the private sector and citizens are fully engaged players that help transform services and innovate for socio-economic development.

Mobile ID deployment should be viewed as a means to an end – a means for citizens to access electronic services that they need and want from the government, private sector or other institution. A holistic approach to m-Services is required and should include the m-ID component.

[3] https://secureidentityalliance.org/

Annex A: Guiding questions for experts

The following presents some of the questions considered during the Mobile ID (m-ID) Expert Group Meeting on 18-19 October 2016. All experts aiming at joining the meeting are kindly requested to follow the structure of their presentation according to the sessions.

1. Overview
    - Overview about eGovernment platforms – one / two slides (e.g. is there one public services portal, open data portal, emergency notification server, identity services, e-signatures services, mobile signatures, interoperability platform, payment services).
    - Overview of legal framework- one slide.
    - Overview of portfolio of ID solutions used by Citizens (like PKI, mID, Token/OTP, Smart Cards etc.) – one slide.
    - Short history of identity development – key dates (e.g. started in 2009) – one slide.
    - m-ID in numbers – statistics about uptake, popularity, transaction per day, average transactions per citizen, popular translation.
    - What were the key success factor for successful m-ID implementation? (e.g. easiness of use, use of current well-known mechanism from citizen point of view).
2. Business model
    - Who pays for what – to whom etc.
    - What are the fees in system?
    - Is the system private-based or public-based?
    - Is there a central hub for e-ID exchange?
3. IT and technical architecture
    - What were the key technical questions that were answered during project?
    - Was the identity solution implementation client-side (on SIM/device) or server-side (e.g. token generated via centralized system)?
    - Was the system build in house or bought from the market? Is the system open-sourced and current code could be reused by other countries?
    - Does m-ID solution use biometrics? Which kind (iris, palm, fingers etc.)? What is the name of biometrics provider (vendor like Fujitsu)?
    - Does m-ID allow to use it in real, physical work or only digital?
    - Is there any central system which logs every transactions?
    - Is every transaction handled by central system? This means that country / system knowns about every transactions (citizen could have problem with privacy)
    - Does citizen has access to his transactions and logs (like where his m-ID was used?)
    - How is m-ID verified? Are there any physical chips or scanners (like in shops) which are used by e.g. Policeman in order to verify m-ID?
    - Does m-ID solution allow to sign a document?
    - Does m-ID solution presents Photo of a citizen? What is the source of photo? (e.g. central national system which is used also for passports)

- Does m-ID allows to verify the verification person (in order to be sure who is verifying citizens)? For example citizen want to make sure that on the other side of transaction there is a policeman
- Does m-ID works offline (without internet)?
- Does m-ID could be verified in offline mode (without internet access due to e.g. certification keys)?
- Does m-ID solution use PIN or password for registration or authorization of transactions?
- Is there any central portal for citizen where he could change his settings?
- Is there any central help desk?
- Where is m-ID data information stored (e.g. does citizen has active m-ID)? Is this national registry?
- Are there any roles in the systems like Policeman could check every data of the profile but drug o shop with alcohol only age?
- What were the advantages of implementing a certain technology over others?
- What are the technicalities and mechanisms of the each solution, especially in the area of authentication and registration (e.g. remote registration based on photos of passport taken by smartphone and send to server)?
- SLA – what are the KPI for service, was there ever any downtime?

4. Security and privacy
   - What are the security mechanism used e.g. in order to assure integrity, authentication?
   - Have the m-ID solution been ever hacked or did somebody tried to hack m-ID? What were the typical attacks?
   - Is there a central certification body? It is public or private?
   - Was there any generated false m-ID on the market?
   - What are the key security requirements for secured ID?
   - How is the m-ID verified during registration (e.g. at Police station, face-to-face)?
   - If m-ID is an app how is it certified and distributed?
   - Is m-ID device paired with m-ID?
   - How privacy is secured for citizens?
5. Mobile ID use-cases and processes
   - Is m-ID used in real, physical world?
   - Is m-ID used in electronic transactions?
   - Whether m-ID is used in public or private sectors?
   - What the most popular services which use m-ID?
   - Is m-ID offered to every citizen including child?
   - Is m-ID used for:
     - Electronic verification at pension funds
     - Postal or bank office (verification by clerk)
     - Building receptions (show ID in order to register)

    - Airports and crossing borders
    - Buying 18+ products (e.g. alcohol)
    - Ski, bike rentals
    - Civic and commercial agreements with banks, insurance etc.
    - Legal procedures in courts
    - Discounts use-cases (show your ID for ticket discount).
  - Please describe high-level processes for registration, first verification and revoking and re-registering for ID
  - Please describe high-level process for transaction

6. Aspect of awareness raising and informational campaign
   - How the rise the awareness about m-ID?
   - What were the main concerns with regards to m-ID (in society)?
   - How were they addressed?
   - What was the societies' response in each case?
   - What stages were the campaigns composed of?
   - What were the strengths and weaknesses of each component?

Annex B – Implementation Examples

The following are the highlights of the presentations made at the Experts Group Meeting. The texts were submitted by the presenters as contributions to this report.

Austria[4][5]

Austrian E-government business model consists of portals at various level (such as general federal, sectoral, regional and local) with services including citizen information, tax payment, social security facilities and health services. A common architecture supported through Open Source Building Blocks, nourished with protocols like XML, SAML, provided the initial push towards e-ID. The timeline of e-ID implementation in Austria begins in November 2000 by an Austrian Cabinet Council decision to adopt chip-card technology to improve citizens' access to public services and to supplement the planned health insurance card with electronic signatures. In February 2003, the first Citizen Card was issued, mass rollouts followed in 2005. In March 2004 the E-government Act was passed in order to provide the legal basis for Identity Management System. From 2005 up to now, several private and public sectors Citizen Card initiatives and both cards, ID and mobile ID started to be utilized.

Mobile ID in Austria is used in about 300 online services in both public and private sectors. Currently there are 700,000 active m-IDs. Card ID amounts to 40,000 health insurance cards and about 80 000 profession's cards (e.g., lawyers, notaries, civil servants). The government continues offering m-ID and card ID to all citizens on a voluntarily basis. Statistics indicate 20,000 daily uses of m-ID whilst that for card ID daily use is not known.

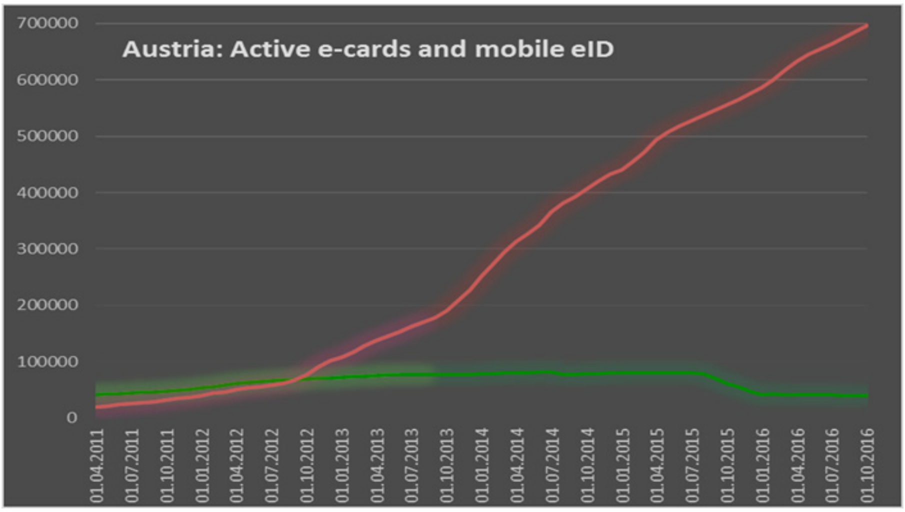
There are several registration procedures for m-ID and card ID including through physical presence and through online secure authentication. Authentication to services using m-ID is either with SMS one time passwords or for smart phones through a QR code protocol. Popular services in public sector are tax, social security and health.

Austrian mobile ID Key Success Factors: Zero footprint and no additional hardware is requested for this implementation and the user only needs a browser. Thus, the system is compatible all Operating systems (OS). It works independently from the mobile phone and mobile network operators (MNOs). By following a server-based solution, no SIM change is required. This also eases activation for citizens. It has low development costs and no cost is applied to citizens.

Austrian mobile e-ID Core Aspects: It is operated by a trusted service provider (TSP) for qualified certificates that manages signature-creation data (cryptographic keys) on behalf of the citizen. The cryptographic keys are operated in a hardware security module (HSM) at the TSP but controlled by the signatory. It has a 2-factor authentication (knowledge & possession) and has a Qualified Signature-Creation Device (QSCD). Austrian e-ID does not use biometrics technology . It has sector-specific identifiers for higher data protection during data transactions.

[4] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/AUSTRIA%2020161018-19%20Austrian%20mID%20-%20ITU%20Warsaw.pdf

[5] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/AUSTRIA%2020161018-19%20Austrian%20mID%20-%20ITU%20Warsaw.pdf



Electronic ID is verified only online and electronically. There were no incidents of hacking into m-ID system and no false activities were generated so far. The supervision body is under state control and a certification body has been notified by the state (according to the EU Signature Directive and EU eIDAS). The security baseline used to be SSCD under EU Signature Directive and now is QSCD under EU eIDAS.

It is expected to meet the level of Assurance of EU eIDAS. During m-ID registration either physical presence at a Registration Office is necessary, along with presenting a photo ID, or alternatives that provide equivalent security and link to previous physical presence allow for online registration (plus e.g. registered letter, a bank transfer).

Awareness raising on e-ID is held through events like conferences or workshops, but also through eGovernment Coordination "Digital Austria" www.digital.austria.gv.at. More information on Austrian m-ID and card e-ID can be found on a portal: www.buergerkarte.at. Advertisements are published or screened in press, radio, websites, and mailings: e.g. inclusion in pension account letters to all citizens by social insurance and integration/mentioning in public sector websites (e.g. tax portal) also support awareness creation.

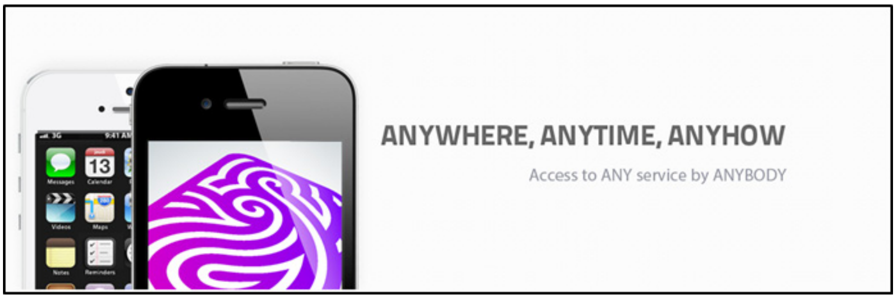
Azerbaijan[6][7]

The first state program on eGov in Azerbaijan was launched in 2003. The first Act on data usage and protection was introduced in 1998 which protected and collected information in Azerbaijan. The country has launched a set of decrees and acts to implement of m-ID. eGovernment portal of Azerbaijan is www.e-gov.az and it works with more than 500 different services and ID use-cases. Mobil ID is closely connected to the eGovernment portal. It provides all necessary information to consumers. "ASAN pay" (www.asanpay.az) is the first nationwide web portal for online payments of fees / penalties imposed by public authorities (traffic fines, court penalties / charges, taxes etc.), private services (public utilities, bank/insurance fees etc.). Citizens can find all necessary information on all payments and fines there.

[6] Presentation available at www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/m-ID%20 Expert%20group/AZERBAIJAN%20Khalilova_Krimpe.pdf

[7] Presentation available at www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/m-ID%20 Expert%20group/AZERBAIJAN%20Khalilova_Krimpe.pdf

Asan İmza (Mobile ID), which means in Azerbaijani language "Simple Signature" has launched as a pilot system in 2013. It became fully operational in 2014 and now all major mobile operators are issuing secure SIM cards.



ASAN İmza (Mobile ID) system is based on the PPP (Public-Private Partnership) model and the partners are the government- all three national MNOs, mobile ID service provider, governmental certification authority and e-service providers. The mobile operator is connected to the whole system through their SIM cards. They issue secure SIM cards and provide end-users SIM-based services, collecting fees for that.

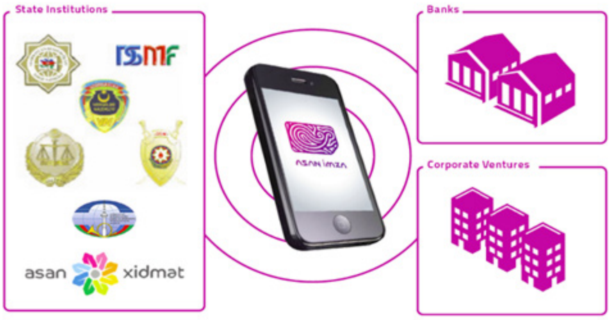
In total, there are 3 main e-service portals which are based on m-ID solution; **e-Custom declaration, Labor and social protection services** and **Tax service.**

Tax services: The Ministry of Taxes is actually one of the first agencies to use e-services in the country, as the volume of work is massive and the automatization adds lots of saving in time and money. Asan İmza (Mobile ID) is actively used in the e-tax operations in Azerbaijan. In 2014, the electronic system of the Ministry of Taxes of Azerbaijan registered almost 6.8 million transactions, 33% of which have been processed by means of Asan İmza (Mobile ID). In 2015, taxpayers conducted around 2.5 million tax operations using their Asan İmza (Mobile ID) via the e-Tax Portal of the Ministry of Taxes.

Labour and social protection services: Starting from August 2014, Azerbaijan keeps a record of employment agreements electronically with the help of Asan İmza (Mobile ID) mobile e-signature service. This innovative service was launched by the Azerbaijani Ministry of Labor and Social Protection of Population, which forced all entrepreneurs and legal entities in the country to conduct all employment agreements with their employees in the electronic system of the Ministry by using an e-signature solution. This concept was introduced with the aim to strengthen the fight against illegal employment as well as to increase the tax and social insurance revenue to the budget. As noted by the Ministry, with this system of e-registration of employment contracts, which is the first of such kind in the CIS region, the government managed to ensure, in a more efficient way, control over the fulfillment of the employment rights in the country. In 2014, the Ministry noted 1.5 million transactions in its e-system whereas in 2015 this figure was around 1 million. The cumulative number of usage e-services of the Azerbaijani Ministry of Labor and Social Protection of Population and the State Social Protection Fund made approximately 1.5 million in 2015.

Customs services: The Azerbaijani customs authorities recently launched the system of e-customs declaration of goods and vehicles imported to the country. The newly introduced e-customs declaration service allows citizens and businessmen to electronically declare their imported goods and vehicles using Mobile ID (Asan İmza) without the need to physically apply to any customs broker / customs department as it earlier used to take place. The whole process is as easy as logging in to the eGovernment Portal using Asan İmza, filling in the e-declaration and signing the ready declaration with again Asan İmza. Within two months (April-May 2016) more than 70,000 declarations have been submitted to customs authorities electronically.

Mobile ID registry is a legal entity online which reduces the registration time from 30 minutes to 1 minute, with the use of ASAN ID. In order to issue the certificate for authentication and digital signing to physical persons for the first time, the client goes to one of the registration centres (State Agency for Public Services and Social Innovations – ASAN Service centers or Centres for Service to Taxpayers of Ministry of Taxes). As a result, the person's SIM card is legally linked to his/her national identity. The registration centres both activate and deactivate digital ID certificates.

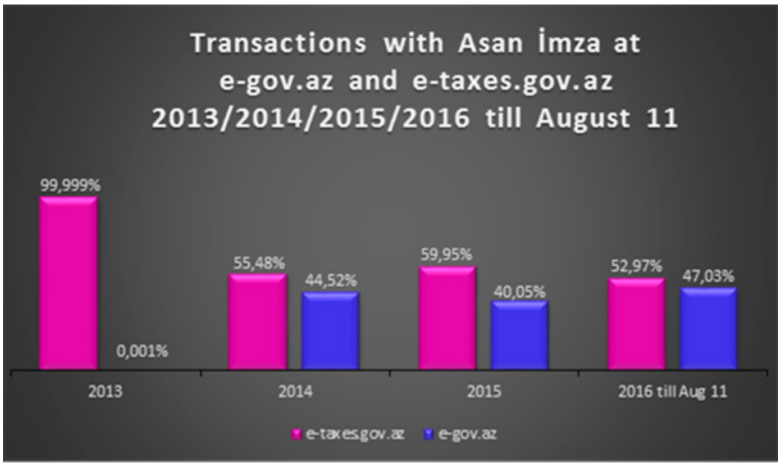


Since the inception of Asan İmza (Mobile ID) service in Azerbaijan, over 250 000 Mobile ID certificates have been issued and more than 15 million transactions were performed with Mobile ID – this is the fastest result of Mobile ID user cases in all over the world and shows the high usability and satisfaction among users. The best indicator showing the success is not the number of issued certificates, but the number of real transactions. During this period over 90% of tax declarations in Azerbaijan were submitted electronically. In general, today over 500 public and private e-services are available to citizens with the help of Asan İmza (Mobile ID) in the Republic of Azerbaijan.

Azerbaijan has areas which are not covered by Internet due to political reasons and some areas have low penetration. Using m-ID saves huge amounts of money of Governmental budget and provides quick progress in development. Most people prefer m-ID to e-ID and it is popular in Azerbaijan to pay taxes and use services. It is easy for younger generation to make transactions through mobile phones rather than tokens or other gadgets.

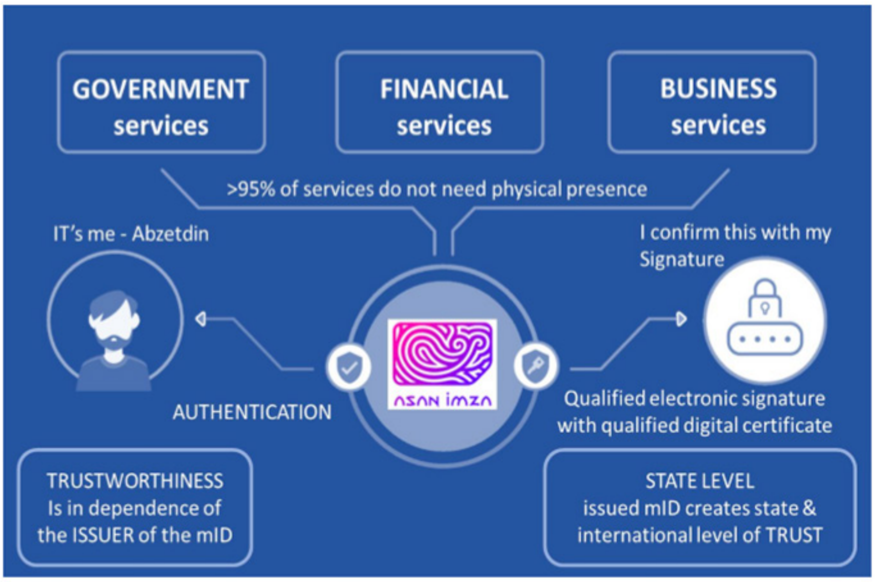
ASAN İmza (Mobile ID) works as a single platform where citizens have pin codes in order to get access to all their services. ASAN İmza (Mobile ID) is the SIM-based digital signature system which is most secure on the market.

Implementing Asan İmza is simple for all parties - customer, operator and e-service provider (who does not need big investments for the technology). Mobile ID is provided as a service-based model. Operators must order new type of SIM cards, issue SIM cards to the Customer and open their SMSC gate for the Mobile-ID service provider. Customers have to get new SIM cards and order PKI certificates. The model is very secure – double authentications are made during the issuance process. First, when SIM is issued by the operator, and second, when certificates are issued by the State Agency. Electronic service providers can integrate Asan İmza into their services very easily using a special toolkit and integration is free of charge. The only necessity is a mobile phone with a secure SIM card. The biggest advantage of this type of m-ID is high mobility and easy usage. It enables using the mobile phone as an authentication and signing tool in a fully secure environment granting access to a wide spectrum of services.



Mobile ID service subscription fee is 10 € (VAT incl.), m-ID service monthly usage fee is 0.5 € (VAT incl.) and m-ID service transaction fee is 0.02 € (VAT incl.). All 3 MNOs provide m-ID service connection order authorisation. Service providers enable bank connectivity to be even quicker and make the content available. Technically, ASAN Imza (Mobile ID) can improve and upgrade its platform and is open for cooperation.

The transaction content is unknown and it is not included in the flow. Authentication and signing transactions are logged in a central system. However, processes transactions logs are stored by service providers. It was integrated into a CA (Certification Authority) portal. Moreover people can obtain access to their personal cabinet with their mID, where they can see the history of all their transactions. It is verified by OCSP from the Certification Authority with no human intervention. ASAN Imza (Mobile ID) uses SIM cards which are evaluated at the EAL5 security level. Signing keys are stored in a secure SIM card which is installed in a mobile phone. The keys are protected by separate PIN codes and users have complete control over them. It can be used for the governmental communication (applet with PKI supports RSA1024/RSA2048/ECC256 encryption) and also with all phones (traditional/simple and smartphones). Everybody is responsible for their own transaction and the system has never been hacked.


GOVERNMENT services
FINANCIAL services
BUSINESS services
>95% of services do not need physical presence
IT's me - Abzetdin
I confirm this with my Signature
asan imza
AUTHENTICATION
Qualified electronic signature with qualified digital certificate
TRUSTWORTHINESS Is in dependence of the ISSUER of the mID
STATE LEVEL issued mID creates state & international level of TRUST

ASAN has added username to avoid spam messaging on mobile numbers and added security pop-up message (verification code). The user can check whether the background action on the device is the same as in pop-up message. This is done in order to be sure that there is no malware or unauthorized movements between certain actions and to avoid clone webs. The client should follow the verification code- they are certified and public. To avoid false and fraud, the citizen has to come to registration authority to receive his m-ID and activate his certificate physically with the use of his passport (face to face physical meeting). The m-ID applet is certified by global SIM card manufacturers and by certification authorities.

The SIM card manufacturer stores the applet into SIMs and distributes physically to related MNOs. Public Key Infrastructure (PKI) solution uses private and public key pairs. Privacy for citizens is secured by Private Key, which is only stored in SIM cards and belongs to citizens. It can't be copied, duplicated or moved out from a chip. Every bank transaction, purchase in e-shop, e-insurance, e-ticket have to be signed digitally. The user has to be over 18 years of age and doesn't have to be Azeri national.

Although, ASAN İmza was developed for governmental services, it also creates many opportunities for the private businesses, whenever secure identification is needed. Therefore, ASAN İmza is like a gateway for modern services in all sectors.

Starting 2015, the financial institutions operating in Azerbaijan such as banks and insurance companies started actively using Asan İmza (Mobile ID) in their activities for provision of online services in a more qualitative and secure way to the customers. During 2015, Asan İmza (Mobile ID) was integrated into the electronic systems of eight leading banks, two payment portals and one insurance company in the country. 10 more banks are in the pipeline for 2016. It is expected that in 2016 all insurance companies will be connected to Asan İmza (Mobile ID) as well. As of today, the Azerbaijani banks use Asan İmza (Mobile ID) in the provision of online banking services such as intra-bank money transfers, currency conversion, payment of loans, payment orders, currency buy/sale/conversion orders, card operations, payment of taxes. Along with the internet bank, some banks started using Asan İmza (Mobile ID) in their internal document flow systems.

The main concerns for the creators are: mentality of people who were not accustomed to electronic services, lack of basic IT literacy skills among general masses (though some layers of the population were quite IT-literate), channels of provision of mobile ID service initially were scarce, the company introduced the mobile ID service to only one mobile operator at the beginning.

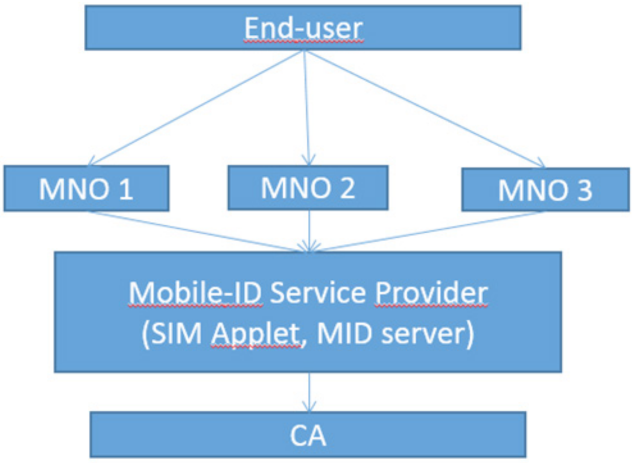
As part of awareness raising, ASAN İmza (Mobile ID) signed an agreement with Islamic Educational, Scientific and Cultural Organization (ISESCO) to incorporate m-ID for the establishment of a single internal document management platform for the ISESCO member states. The platform, titled as "ISESCO BESTDOC PORTAL", will be functioning on the basis of a unique digital identity tool – ISESCO ID, designated specially for ISESCO based on the Azerbaijani technologies of electronic and mobile identity – "Asan ID" and "Asan İmza", and will provide an opportunity to ISESCO member states to interact within single e-environment aiming to improve the process of document workflow.

Though Azerbaijan is a country with high level of mobile penetration in the region, yet people still trust traditional paper documents and are not ready to go fully digital. Azerbaijan is among a few countries that uses m-ID and young generations are involved in this process. The company tries to explain to users on all social media how to use and be part of mID. The priority for ASAN İmza is the promotion of m-ID to people and seeking foreign investments. The trend shows that people who use m-ID never return to e-ID. Many celebrities are involved in promoting mID. The creators believe that the positive experience of each person interacting with e-services and mobile ID technology will "infect" others and bring them to the mobile ID users community of the country.

Estonia[8][9]

The work on e-ID in Estonia started in 2000 and the first ID card was issued in 2002. ID card is a mandatory document in Estonia. The card was initially not popular but the country continued to work on it. By now, 1,277,212 active ID-cards are on the market and there are more than 500,000 active users who effect more than 18 million e-ID transactions every month (authentication and digital signing). Mobile-ID was introduced in 2007. At the same time there are also 100,000 Mobile ID users. On one hand Estonia has Digi-ID, which is a chip card for digital use only and on the other, ID-cards for physical identity. If the ID card is lost, the citizen can go to the police and apply for Digi-ID card and get it within 30 minutes. All IDs (ID-card, Digi-ID, and Mobile-ID) have PKI certificates for digital signatures and secure authentication. All private keys are stored on chip or SIM card. Mobile-ID users are more active and they makes more transactions than e-ID users. 99% of banking transactions are online. More than 30% of citizens vote online and 98% pay taxes online. E-prescription is also a service used in 99%. Different partners who are involved with Mobile-ID are MNOs.

Initially all MNOs had their own technologies and different SIM applets. Since 2014, there is a centralized Mobile-ID service provider and Mobile-ID is still SIM based PKI solution. PKI private keys are stored on the SIM card. Mobile-ID works as a single sign on solution for all e-Service providers and government services. The enrolment process is the most critical part, face to face verification is done, and the process is trusted by all parties of the ecosystem.



Secure keys are stored on the SIM card and the Mobile ID customers' private key is under their control. Messages to and from SIM are encrypted and decrypted only for the mobile user to see. The Certification Authority (CA) keeps secure logs about the PKI side and PKI certificates (RSA2k, ECC) are used in m-ID in Estonia as a warranty of security and privacy issues.

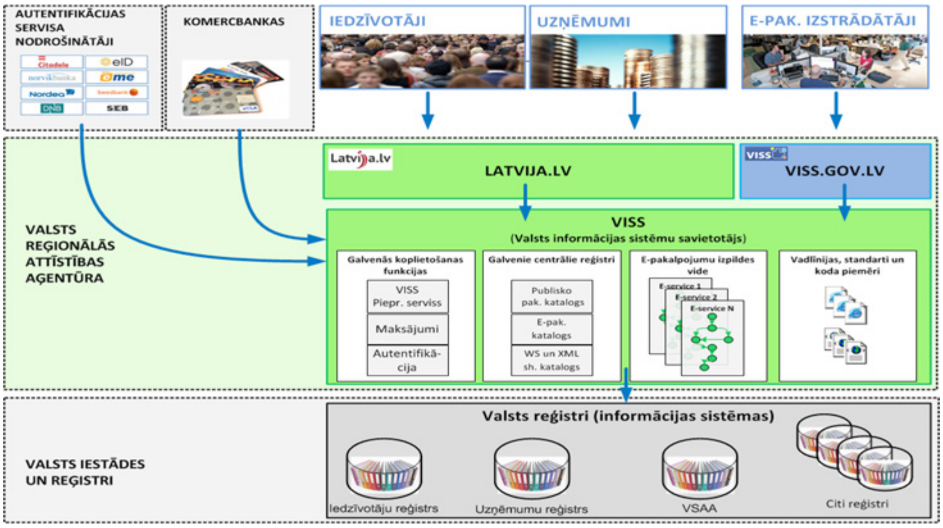
Today, most of the issued SIM cards are Mobile-ID ready by default. The solution is available for all citizens above 16 years of age and it is for digital use only. Subscribers have to pay €1 per month having a Mobile-ID. 3 million Mobile-ID transactions per month are conducted in Estonia. There are currently over 100,000 mobile ID users. Moreover mobile-ID is more convenient than e-ID cards. The main concern in Estonia is to have more than 500,000 active ID-card users and to change peoples' habits to start using Mobile-ID. All e-ID software are open-source and free of charge for end-users and e-Service providers to integrate with their own services. For citizens there is free of charge desktop software to sign documents digitally and verify signatures.

[8] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/ESTONIA%20Presentation%20for%20mID%20expert%20group.pdf

[9] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/ESTONIA%20Presentation%20for%20mID%20expert%20group.pdf

Latvia[10][11]

Right now Latvia doesn't have any m-ID solutions, but has plans on m-ID implementation in their roadmap.



The main platform is called e-Government and includes the following:

- public services portal
- identity service
- e-signature service
- mobile signatures
- interoperability platform
- payment services

In 2006 Latvia issued the first electronic signature card. In 2012 the country issued its first e-ID card with authentication and e-signing function and in 2017 the development of m-ID will commence. Around 95% of the user population don't understand difference between of m-ID and e-ID solutions, which makes it a big challenge for government. Security and privacy issues dealing with m-ID implementation is a concern. A common trend among citizens is that they don't need mID, e-ID nor authentication and esignature. It is important that they receive the right services for a successful rollout. m-ID is currently on the government's agenda. Raising awareness on m-ID implementation will be held in Latvia with campaign in all states and private organizations.

Malaysia

The Malaysian identity card is the compulsory identity card for Malaysian citizens aged 12 and above. The current identity card, known as MyKad, was introduced by the *National Registration Department of Malaysia* since September 2001 as one of four Multimedia Super Corridor (MSC) Malaysia flagship applications and a replacement for the High Quality Identity Card. Mykad is a multi purpose smartcard incorporating a variety of applications from various government agencies and the private sector. The

[10] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/LATVIA_Warsawa_event_v05%20%281%29.pdf

[11] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/LATVIA_Warsawa_event_v05%20%281%29.pdf

MyKad stores information on name, address, race, citizenship and religion as well as stores finger print minutiae in a smart chip. Finger print verification may be done accurately remotely using a MyKad reader.

MyKad is mainly used as a validation tool and proof of citizenship other than the birth certificate, However it also contains applications that may be activated by the bearers of MyKad which includes an electronic purse and a public key. MyKad is issued by the Malaysian Government free of charge.

The Public Key Infrastructure (PKI) application incorporates digital certificates and personal key inside MyKad. The digital certificates allow transactions to be done electronically for verification and authentication.

The public who wishes to enable MyKad to function as a digital certificate may contact any of the Certifying Agencies (CA) licensed by the Malaysian Communications and Multimedia Commission (MCMC). PKI application is widely used by Malaysians amongst others for on-line filing of their annual tax returns to the Inland Revenue Board (IRB), import and export permit application as well as participation in Government electronic procurement. To use the MyKad PKI, the users would have to first register at the website of any licensed certificate authority (CA) to request for a digital certificate online. Upon registration, the user may use his/ her MyKad PKI for encryption and/or signing.

Apart from the above applications, MyKad has embedded an electronic purse application known as Touch n Go that uses contactless technology. Thus value can be stored in the Touch n Go application in MyKad for payment of toll fees at highway toll plazas, light rail transit train tickets and so forth.

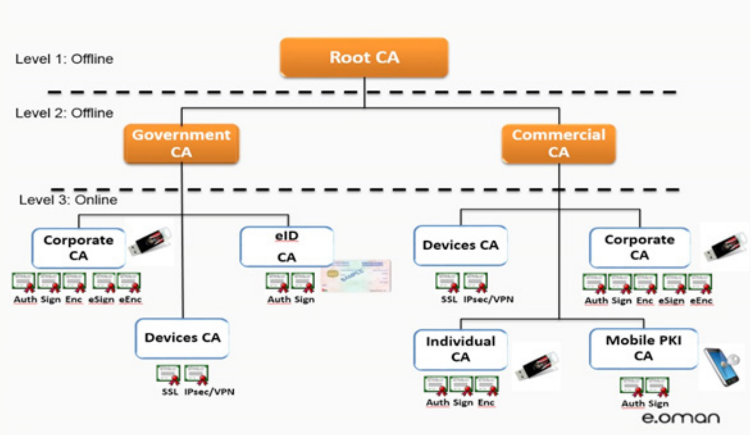
To prepare the citizens to participate actively in the digital economy, Malaysia is looking into enhancing further the trust factor to ensure that the public can transact with ease, confidently, securely and their privacy protected through the implementation of digital identity. One of the considerations is to leapfrog Malaysia towards mobile identity leveraging on the MyKad, infrastructure and various available channels. Currently, work on development of an appropriate framework and legal requirements are being studied as well as engagements with the public and private sectors are being carried out to obtain feedbacks and inputs on the optimal business model, technical considerations and cost effective approach for Malaysia which would encourage public adoption of government online services, e-commerce and critical digital services offered by the private sector. \

Oman[12][13]

In the Sultanate of Oman, the eOman Strategy is the roadmap of the national project of government services transformation from paper based to absolute online services using PKI strong authentication and electronic signature. One of the main priorities was to have a National PKI (Public Key Infrastructure) and the work is being continued since 2008 starting by declaring the Electronic Transaction Law 69/2008 including PKI services. In order to achieve this, it was necessary to define and develop the policies, process and procedures. Oman has the physical capabilities to allocate human resources needed for this project which was started in November 2011 by ITA (Information Technology Authority). In July 2013, Oman announced to the world that the Oman Nation PKI is live with a Root CA (Certificate Authority), two intermediates CAs and seven subordinate CAs as illustrated.

[12] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/OMAN%20%20Mobile%20PKI%20%28Mobile%20ID%29.pdf

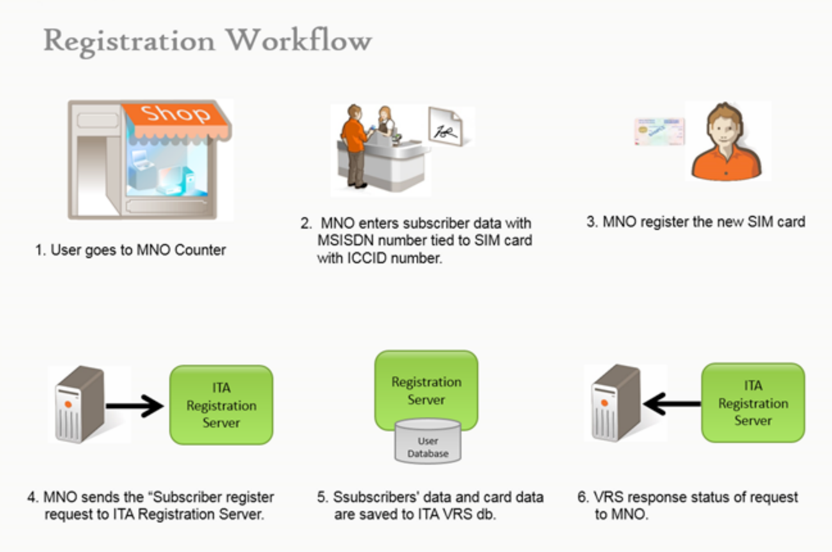
[13] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/OMAN%20%20Mobile%20PKI%20%28Mobile%20ID%29.pdf



Along with PKI project implementation, the government headed by ITA announced the readiness assessments of e-services as 80:20 Plan (20% of critical entities provide 80% of government services) and hence the work started to reengineer the business process of those 20% government entities and then to develop the electronic services and web portals aiming to ease the use of online services and avoid the physical presence in the services providers' premises. Oman National PKI aimed to increase the number of e-services of Government and private entities, and effectively engage in government transformation by granting the following:

- Electronic transaction protection against identity fraud
- Data integrity, data confidentiality, strong authentication, and non-repudiation
- Trust, confidence and easiness to use online services for citizens and residents

It increased the level of confidence to exchange information over Internet through the use of public and private cryptographic key pairs. Moreover, the PKI in Oman leveraged data protection as it is compliant with e-transaction laws 69/2008. Oman National PKI is owned and operated in ITA by National Digital Certification Center (NDCC) which provides PKI services to organizations and the public. PKI is not only technology but also about policies, standards, procedures and people. All citizens and residents get PKI certificates which is by default embedded in the National ID card. The m-ID solution chose top two mobile operators (first licensees) and accredited each of them to be as a registration authority (RA) to have our PKI services.


Registration Workflow
Shop
1. User goes to MNO Counter
2. MNO enters subscriber data with MSISDN number tied to SIM card with ICCID number.
3. MNO register the new SIM card
ITA Registration Server
4. MNO sends the "Subscriber register request to ITA Registration Server.
Registration Server
User Database
5. Ssubscribers' data and card data are saved to ITA VRS db.
ITA Registration Server
6. VRS response status of request to MNO.

ITA is reaching out to people and organizes the PKI awareness campaign. Oman doesn't allow many service unless authentication is done successfully.

Poland

The polish government is currently developing a roadmap for m-ID and is currently at the stage of establishing international comparison of approaches towards implementation of m-ID and e-ID.

Poland does not currently provide citizens with electronic identity card with chip. For now, the only public, free of charge tool for electronic identification and authentication of citizens used for dealing with the public administration is the Trusted Profile (Profil Zaufany).

Poland is concurrently developing a national strategy for digital identity. The basic idea is to provide citizens with a federated identification system, allowing use of services from various providers from private (e.g. banks, telecoms, postal) and public sectors. Implementation of the system is based on two major projects: e-ID and mDocuments (mID).

The e-ID project consists primarily of:

- Implementation in 2017 of a domestic node, acting as Identity Broker for eGovernment services
- Cross-border node implemented on production with CEF financing
- Open-source code and involvement of banks credentials in the process of registration of public ID
- Electronic signature (Trusted Profile, implemented in Poland in 2011)

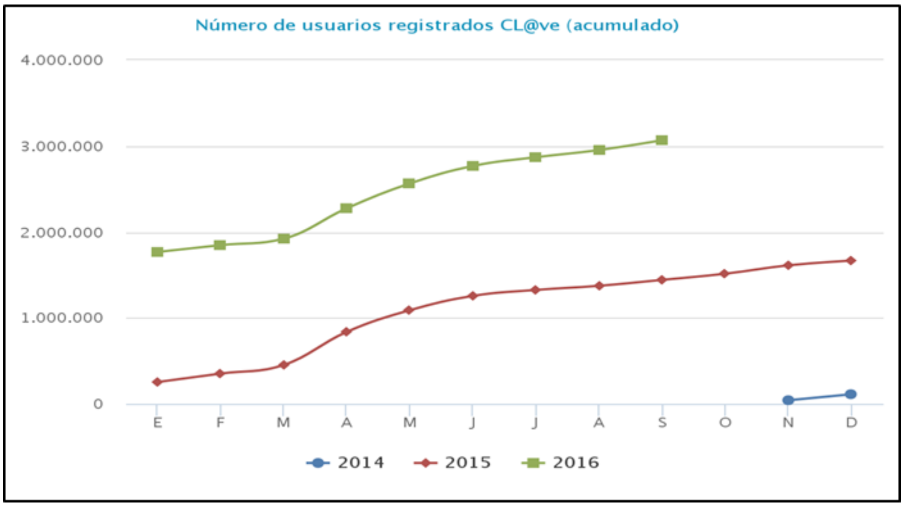
The implementation of mDocuments (mID) project will equip citizens with a new, credible and optional mechanism for presentation and confirmation of their identity. The realization of the vision of the electronic presentation of identity documents for citizens is possible through the use of services of Polish eGovernment which allows to display the documents in electronic form sources in the System of National Registers or other reliable databases and systems. This approach enables to offer e-services also on older mobile phones which are not smartphones. The mDocuments project has been divided into phases. Implementation of the first phase, which will take place in 2017, will offer the citizen an m-ID card. In the second phase, citizens will be provided with mDriving License, mVehicle registration certificate and vehicle mInsurance. The third phase of the project is scheduled for the beginning of 2018. It is expected that new e-services will be launched or already existing e-services will be used, which will enable citizens to access more the documents electronically.

Spain[14][15]

In 1999 CERtificación ESpañona - Spanish Certification (CERES) launched a project called PKI-FNMT and made it possible to hand in annual tax declaration online with an electronic certificate. The same year the government introduced a Directive 1999/93/EC Electronic Signature and in 2003 the Electronic Signature Law and Certification Services Provider market regulation has been announced. Before 2006 Spain had independent applications and user registries. Since 2016 Cl@ve project is issuing a digital signature on the cloud. Mobile ID in Spain is currently under implementation. Spain has a series of services and a web page on mID. Since 2006 Spain has mobile applications and initiated e-document processing.

[14] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/SPAIN%202016%2010%2011%20guiding%20presentation%20for%20mID%20expert%20group.pdf

[15] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/SPAIN%202016%2010%2011%20guiding%20presentation%20for%20mID%20expert%20group.pdf



The Cl@ve project has enabled an authentication mechanism adapted for mobile devices and mobile identification. Registration is 100% online and use of digital certificates on smartphones is also possible. Electronic Certificate validation broker (@firma) is provided to all public sector by the Ministry of Finance (DTIC): SaaS. @firma is the name of the platform that validates all digital certificates (300.000.000 validations each year). If a Ministry (e.g. Ministry of Justice) has a high demand, a specific installation of the software (@firma) is done in their infrastructure instead of using the datacenter facility. This installation is called "federado"= federated. If heavy use is demanded then single installation is needed (@firma_federado). Central administration pays SW development and maintenance: Cl@ve (both Cl@ve and @firma developments are paid by central administration). The public CA doesn't charge citizens, but it receives money from government. Simpler technologies help to citizens access electronic administration more easily, which then uses federated different assurance levels which are possible using passwords and authentication tokens without the need of digital certificates. SMS PIN or SMS PIN + password. Those are two ID schemas of Cl@ve: single factor or double factor systems 100% managed by Public Services. CAs can be private but by law, requires a 3,000,000€ insurance policy. The main concern is the use of Digital Public services which was low in spite of the fact that most of the citizens use smartphones. Awareness raising in Spain is held mainly during annual tax declaration periods.

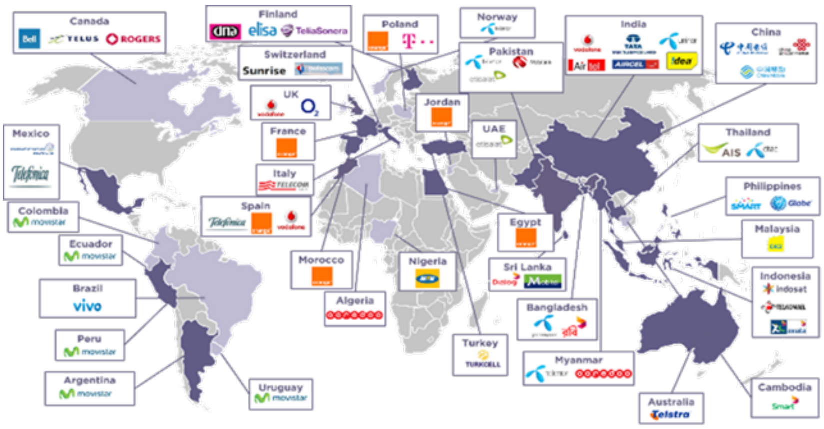
GSMA[16][17]

Mobile Connect is the mobile operator which facilitates authentication and identity service and provides simple, secure and convenient access to online services from any device in different countries of the globe. GSMA has its services in India, China and countries in Africa, Europe and Asia. It launched identity services and m-ID implementation recommendations in UK and China. It combines the users' unique mobile number and an optional PIN for added security, to verify and authenticate the user everywhere they see Mobile Connect which is the new product of GSMA. Mobile Connect of GSMA has grown at an exceptionally rapid pace and today is available to more than 2.8 billion mobile users. Mobile Connect is interoperable for any country and accessible to any country. This service does not require knowledge of the name of the user. Mobile Connect is a secure universal log-in solution. Simply by matching the user to their mobile phone, Mobile Connect allows them to log-in to websites and

[16] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/GSMA%20Expert%20Group%20Meeting%20on%20Mobile%20ID%20-%20Poland%2018Oct16.pdf

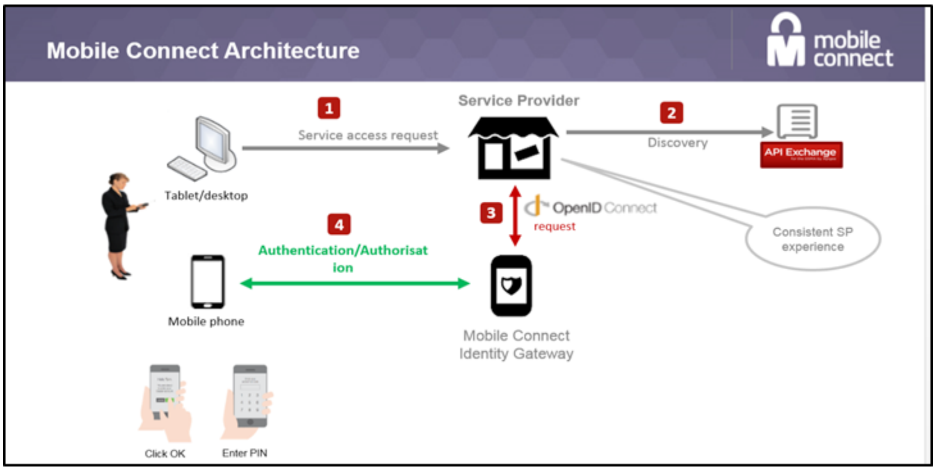
[17] Presentation available at http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/mID%20Expert%20group/GSMA%20Expert%20Group%20Meeting%20on%20Mobile%20ID%20-%20Poland%2018Oct16.pdf

applications quickly without the need to remember passwords and usernames. It is safe, secure and no personal information is shared without permission.



In general, Mobile Connect brings benefits like:

- Simple user experience, on a mobile device.
- Frictionless login encourages citizens to access government services more often.
- Flexible security helps protect citizens' accounts and personal details.
- Compliant with regulatory requirements on authentication, aligned with international security standards.
- Outspoken privacy focus preserves citizens' trust and aligns with government priorities.
- Cost effective, no need for additional devices or readers.
- Efficient and ubiquitous solution, working across public and private sector.
- Enables new digital public and private services thus improving citizens' daily life.



Mobile Connect Architecture

mobile connect

1 Service access request

Service Provider

2 Discovery

API Exchange

Tablet/desktop

3 OpenID Connect request

Consistent SP experience

4 Authentication/Authorisation

Mobile phone

Mobile Connect Identity Gateway

Click OK

Enter PIN

Easy-to-use digital identity is a key enabler to build a more connected society and enhance digital inclusion. Mobile operators are already working with digital service providers, hence are the ideal partners to create a trustworthy ecosystem. Drives scale and ensures national and international inter-operability.

References

1) www.securitydocumentworld.com/creo_files/upload/article-files/GlobalPlatform_White_Paper_MobileID.pdf

2) www.jpn.gov.my/en/informasimykad/off-card-applications/

3) www.digital.austria.gv.at

4) www.buergerkarte.at

5) https://www.e-gov.az/en/content/read/14

6) https://e-estonia.com/component/mobile-id/

8) http://id.ee/index.php?id=37325

9) www.itu.int/ITU-D/cyb/app/m-gov.html

10) www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2016/mID/Expert-Group-Meeting-on-Mobile-ID.aspx

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Office of the Director
Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and
Director，Administration and
Operations Coordination
Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling
Environmnent and
e-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership
Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge
Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication
Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

Email: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des
télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Bureau de zone
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication
Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de
Telecomunicações (UIT)
Regional Office
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU)
Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Arab States

Egypt

International Telecommunication
Union (ITU)
Regional Office
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Email: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia and the Pacific

Thailand

International Telecommunication
Union (ITU)
Regional Office
Thailand Post Training Center, 5th
floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

CIS countries

Russian Federation

International Telecommunication
Union (ITU)
Area Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Switzerland

International Telecommunication
Union (ITU)
Telecommunication Development
Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5111

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-24611-2
9 789261 246112

Printed in Switzerland
Geneva, 2017