The world is going mad for mobile

Are government-sponsored ID implementations keeping up?

Joint whitepaper by
The SILICON TRUST and Infineon Technologies

www.infineon.com/mobileID

Abstract

Mobile technologies have been a game changer in every aspect of our daily lives: tracking down information, making payments, accessing services, playing games or using a vast amount of other applications in a flexible manner. It's therefore natural that interest in mobile ID implementations is rising. In this paper, we examine what mobile ID is, the driving factors behind it and some of the challenges of public sector implementations.

Demand for the convergence of mobile and ID technology is driven by significant developments in the business, technology and consumer worlds: we want speed, security and convenience when we access our bank accounts, pay for goods, use mobile ticketing, interact with the authorities, or log on to our workplace systems.

According to the research firm IHS Technology, an estimated number of 2.2 billion NFC-enabled handsets will be shipped in 2020, mainly driven by payment applications such as Apple Pay, Alipay and Samsung Pay. [1]

Mobile payment transactions are already popular, and continue to rise steadily. A report about consumer-friendly technology published by the British Bankers' Association (BBA) and Ernst & Young (EY) in 2014 reveals that mobile and Internet banking is being used for transactions worth nearly one billion GBP a day in the UK alone.

The banking apps for mobile phones and tablets required to make these transactions had been downloaded more than 14.7 million times at the time of the report, at a rate of 15,000 downloads per day. Banking by smartphone and tablet has also become the leading way for customers to manage their finances, according to a 2015 survey by CACI for the BBA. By 2020, the report forecasts that customers will use their mobile devices to manage their current account 2.3 billion times – more than traditional Internet, branch and telephone banking service usage numbers put together. [2]

The Silicon Trust is a partner program promoting the use of silicon-based security. With over 30 partners, the Silicon Trust has been an active influencer of the ID industry for over 15 years.

Infineon is the leading provider of security solutions and offers tailored and ready-to-use security solutions serving a wide range of applications from smart cards to new, emerging IoT use cases. Outstanding security expertise and technology innovation based on almost 30 years of experience, system competence and the broadest security solution portfolio focused on customer needs is what makes Infineon the preferred security partner.

Contents

1. What do these statistics in mobile transactions mean for the world of ID?

These developments demonstrate that consumers are using their mobile devices for so much more than just voice communication. The mobile device has become the preferred access point to online services across many sectors, a trend which governments can tap into. It is understandable, therefore, that using mobile technology for identification is the next logical step for governments around the world, who have migrated over the past 100 or so years from printed paper to laminated plastic card and latterly to two-factor, smart card-based ID.

Governments are under a lot of pressure to digitize their administrations, remain attractive to their workforce and ensure that a majority of public sector services are accessible online. Mobile technology plays an increasingly large role in the modernization of administrative processes, both internally, for the civil servants themselves, as well as for the delivery of online services.

2. What is the basic technology behind mobile ID?

Generally speaking, mobile ID refers to a mobile-based secure authentication solution, which, in the case of government applications, can be used to securely identify a citizen.

Using a mobile ID solution has the potential to increase the take-up of online services by a country's population radically. In this instance, governments include mobile accessibility into their digital strategies. Such strategies enable mobile devices to be used for identity verification instead of using traditional forms such as ID cards or badges. When implemented well, mobile ID delivers security and convenience by using mobile-based authentication and consent-based digital identity management. It can be issued as a substitute for a traditional physical ID card or it can be derived from one that's already been issued.

Mobile ID authentication solutions are usually Public Key Infrastructure-based and can take up different forms, such as:

1. SIM-based mobile ID: Data is physically stored on the SIM card of the mobile device.
2. Embedded mobile ID: Relevant identification data is stored in the embedded secure element (SE) of the handset.
3. NFC-based mobile ID: This solution uses the contactless NFC interface of the mobile device to securely access identity and authentication information from an external token, e.g. a smart card.
4. Server-based mobile ID: In this approach, secured identity and authentication information is stored on an external server, which can be accessed using a handset.
5. Derived mobile ID: A derived mobile ID is a special form of mobile ID. It can take up different forms such as SIM-based or embedded. A derived mobile ID is mostly set up from an ID card by deriving credentials; the ID derivation enables the use of new technologies, being in fact a technical extension of an existing eID with the same high level of assurance.

What is a derived credential?

The term “derived credential” was coined by the US National Institute of Standards and Technology (NIST) to refer to credentials carried by employees in Personal Identity Verification (PIV) cards and Common Access Cards (CAC). Today, the term usually refers to credentials carried in a mobile device that are derived from primary credentials stored in a smart card. The derived credentials are functionally equivalent to the primary credentials. Derived credentials are created by a device registration process that does not need to duplicate the high assurance procedures for identity proofing as performed for the issuance of the primary credential.

To overcome the problem of a verified mobile device being lost or stolen, and being obtained by thieves who could then access government information because they possessed both an access point and a security token, derived credentials can be set to expire fairly quickly after use.

Today, derived credentials can already be used in various scenarios, e.g. to sign an email, for user authentication, or for making payments, e.g. Apple Pay.

3. Security aspects of mobile ID

Smartphone security infrastructure

The security behind any mobile ID solution must work with the security infrastructure of modern smartphones. GlobalPlatform defines the security framework as made up of three environments, each with a different task. Depending on the application, a mobile ID solution will incorporate these specific environments:

- **Rich OS (Operating System):** An environment created for versatility and richness where applications run on operating systems such as Android, Symbian and Windows Phone, for example. It is open to third-party download after the device is manufactured. Security is a concern here, but is secondary to other issues.

- **TEE (Trusted Execution Environment):** The TEE is a protected area of the main processor in a smartphone (or any connected device) and allows sensitive data to be stored, processed and protected in an isolated environment. The TEE's ability to offer isolated, protected execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights.

- **SE (Secure Element):** The SE is a secured component, which comprises autonomous, tamper-resistant hardware within which secured applications and their confidential cryptographic data (e.g. key management) are stored and executed. It allows high levels of security, but has limited functionality and can work in tandem with the TEE. The SE is used for hosting proximity payment applications or official electronic signatures where the highest level of security is required. The TEE can be used to filter access to applications stored directly on the SE to act as a buffer against malware attacks. [3]

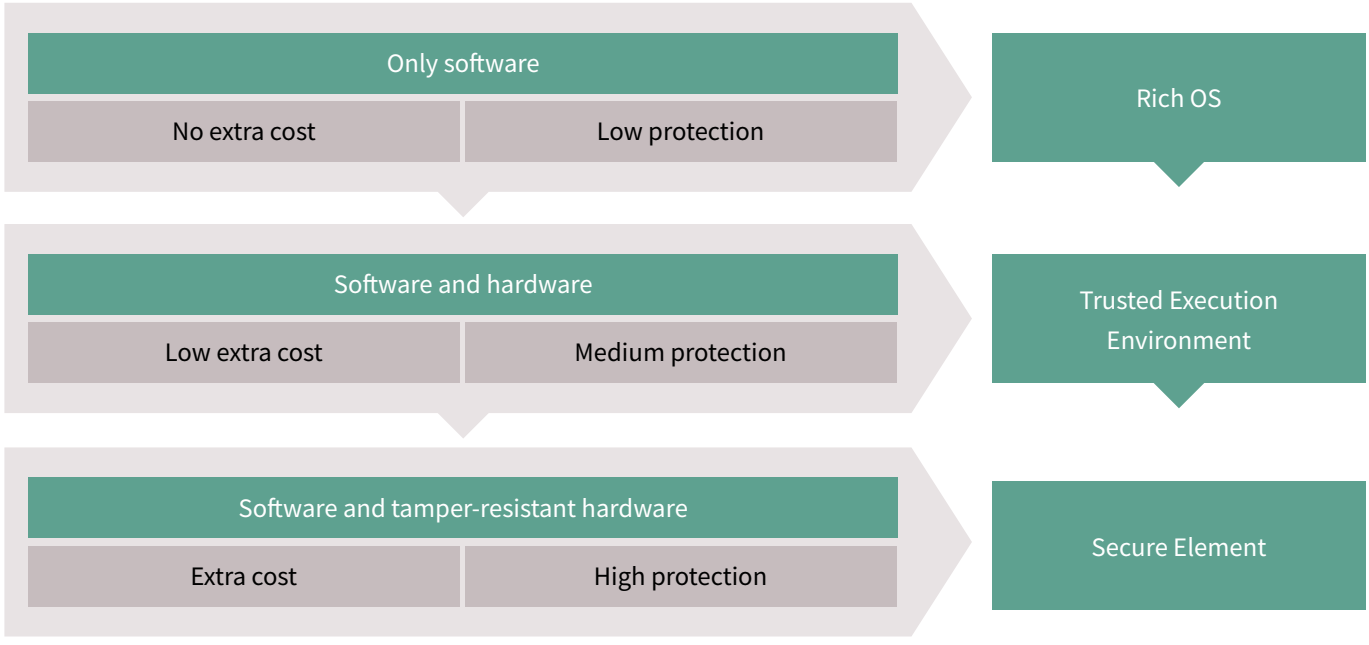

FIG 1: Specific security environments (Source: GlobalPlatform)

Visualizing security for the consumer

With such a wide range of government applications – from residence registration to checking pension entitlements, determining and assuring the appropriate security level is key to the success of any implementation. With this in mind, Infineon and the Silicon Trust believes that Europe needs trusted and interoperable security products and services and that these products should be compliant with European directives and regulations. Three main pillars that are the basis of these considerations are: interoperability, which is based on standardization; trust, which is based on coherent and transparent processes; and assurance, which is based on independent evaluations and certifications.

The challenge for any system establishing security levels in the cybersecurity sector is that it needs to cover a wide range of ICT (information and communications technology) products and services while, at the same time, meeting the needs of different risk levels. With such a wide range of security threats that need to be addressed, regulations also have to keep in mind the industry's need for scalability, flexibility, cost effectiveness and fast time-to-market. There would be very little use in a security level matrix that cannot balance technology and industry needs with the requirements of individual application areas.

The Silicon Trust and Infineon support the EU Security Labeling Proposal, which is designed to visualize the security inside the proposed solution. This approach will help both the industry and the implementers to illustrate the security level applied, thereby increasing transparency.

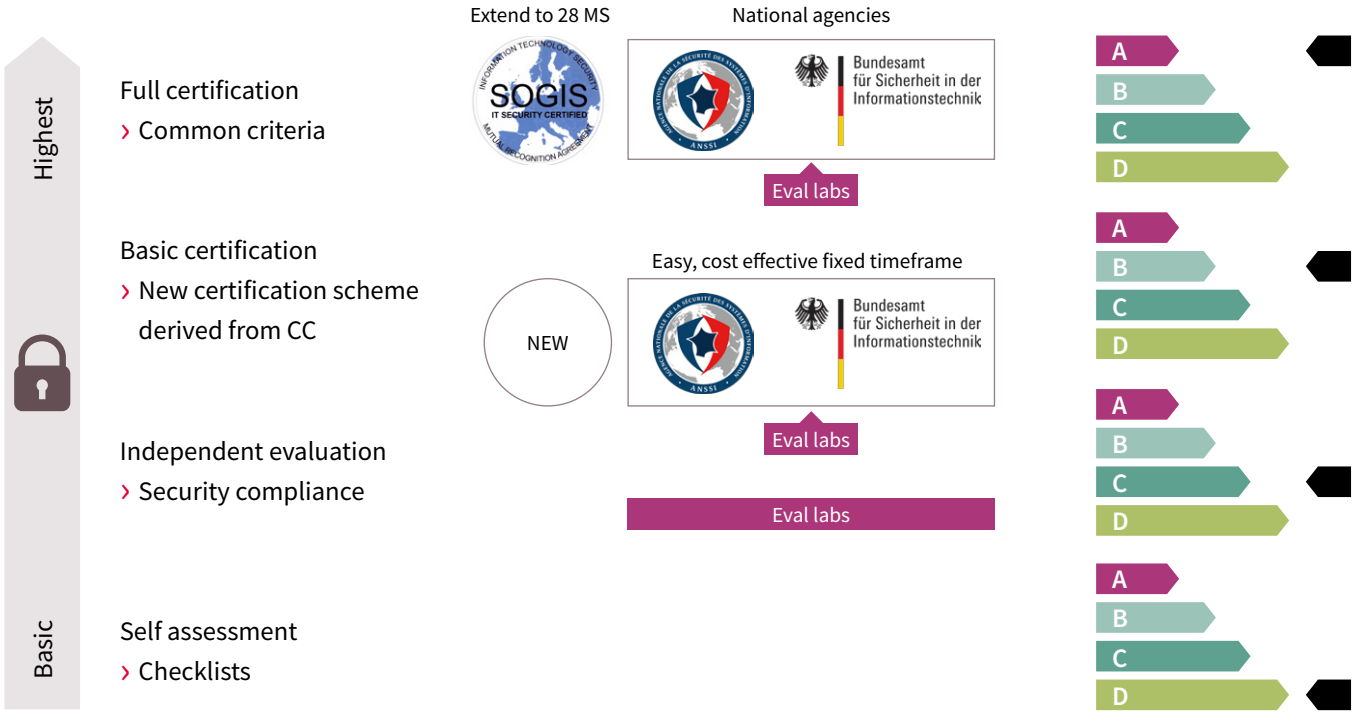

FIG 2: EU security labeling proposal by Infineon and STM

4. Parallel developments and disruptive technologies

If we take a step back from the technicalities of national schemes and look at the take-up of mobile applications in other sectors, it reminds us just how willing the general public is to use mobile devices to authenticate, to pay, or to travel.

Apple Pay, Alipay, Android Pay, and Samsung Pay are increasing the formats in which consumers can make payments – both in store and using apps. There has been a big hype around these technologies and the users of these payment technologies have given them rave reviews. However, these systems still need to make the move to serving mainstream consumers instead of early adopters only.

Apple Pay
When making contactless in-store payments with their default payment card, Apple Pay users rest their finger on Touch ID and hold their iPhone towards the contactless reader until the transaction is successful (a fairly similar approach is also taken using the Apple Watch). If they want to use a different payment card, they hold their iPhone to the reader without resting their finger on Touch ID. When the default card appears, they tap it, then they tap the one they want to use and rest their finger on Touch ID to pay.

Touch ID
Apple's Touch ID relies on a fingerprint recognition sensor that is available for all newer device models starting from the iPhone 5S and newer iPad models. Touch ID is heavily integrated into iOS devices, allowing users to unlock their device, make purchases in various Apple digital media stores, and to authenticate Apple Pay online or in apps. Fingerprint information is stored locally rather than remotely on Apple servers or iCloud, making it difficult for fraudsters to access.

One of the most well-known mobile-based applications is the taxi ride app Uber, which was founded in 2009. It's now available in 70 countries, 400 cities and boasts more than 15 million active users – per month. The core aspect of Uber's massive success is the – albeit low in terms of security – level of identification for driver and passenger, as well as the fast and in-app payment options. In the cities where it operates, users can use the Uber app to request a ride and receive information on timings and the driver. When users arrive at their destination, the fare is automatically calculated and charged to the payment method linked to their account. The app is also integrated with Apple Pay in a feature known as Ride Now, which enables users to pay for their ride using Touch ID. The process means that if users have an eligible credit card already added to Apple Pay, they don't need to enter it again to pay for their Uber ride. Instead, they simply place their finger on the Touch ID sensor of their iPhone.

Even Germany, a country with little or no contactless or mobile payment market, has embraced the mobile for taxi rides. With 10 million users, the German taxi app MyTaxi uses in-app payment as a standard option. This may seem far-fetched for mobile ID in national schemes, but it shows that the user is willing to use a mobile device for security-sensitive transactions if the combination of ease-of-use and added value is given.

Concerning identity checks in the private sector, the UK-based start-up Yoti is positioning itself to solve the challenge of proving one's identity in the digital world. Using its scheme, users enroll for a digital identity (known as a Yoti) using a smartphone app. Facial recognition is used to score biometric reference and 'selfie' image, enabling the user to prove their age and log in to new websites.

Another app based on selfie technology is Mobile Passport Control (MPC) in the US. The MPC app from US Customs and Border Protection (CBP) is the first authorized app to expedite a traveler's entry process into the US. Airside Mobile and the Airports Council International-North America (ACI-NA) developed it in partnership with CBP. Eligible travelers with a smartphone or tablet can download the MPC app from the Apple App Store or Google Play Store and create a profile, which includes their name, gender, date of birth and country of citizenship. On landing in the US, they can complete a 'new trip' section by providing details of their arrival airport and airline, taking a selfie and answering customs declaration questions. Once the form is submitted through the app, the traveler receives an electronic receipt with an encrypted Quick Response (QR) code, which is valid for four hours. Travelers then bring their passport and mobile device with their digital barcoded receipt to a CBP officer to finalize their inspection for entry into the United States.

The convenience, ease-of-use, and security of apps such as Uber and MPC are encouraging more citizens, businesses, and governments to move towards using mobile devices for identification and authentication. This could provide motivation and guidance for government-initiated mobile ID schemes.

5. The European angle on mobile ID

Today, mobile devices are the gateway to every part of our lives. According to the GSMA's The Mobile Economy 2015 report, smartphone adoption is already reaching critical mass in developed markets, with the devices now accounting for 60% of connections. In an ever-connected world, where public and private sector services are becoming more digitized, there is a growing need for privacy and protection of electronic identities to make it easier and safer to use digital services. [4]

The mobile device can work as a terminal and gateway for citizens to interact with governments and businesses to access services. However, a predictable regulatory environment for electronic identity and trust services is key to promoting global interoperability. Governments will play a central role in supporting the private sector's development and adoption of strategic partnerships in the digital identity ecosystem, and there will be more collaboration between the public and the private sector.

eIDAS

As businesses and governments move towards providing multi-channel services, the need for new trustworthy digital means of authenticating and signing is becoming more pressing. With this in mind, Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) has been devised. This regulation replaces the EU signature directive of 1999 and national laws on eSignatures, and establishes an internal European market for cross-border transactions. Between 2014 and September 2015, a series of implementing acts were completed in preparation for the regulation coming into force on July 1, 2016, when the rules for trust services started to apply. The mandatory mutual recognition of eIDs will apply from September 2018.

eIDAS aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It allows people and businesses to use their own national eID schemes to access public services in other EU countries where eIDs are available. In turn, this means that electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication work across borders and have the same legal status as traditional paper-based processes.

These foundations mean that 'one-click' transactions and services can be accessed securely, such as remotely opening bank accounts, setting up a business, authenticating Internet payments, or enrolling at a foreign university. As a result of this regulation, from September 2018 EU member states will have to recognize and accept any EU-notified means of electronic identification. This means that two parties in any of the EU member states can enter into a legally binding agreement digitally in seconds. Furthermore, eIDAS will enable organizations throughout the EU to cut costs and improve efficiency.

eIDAS overview

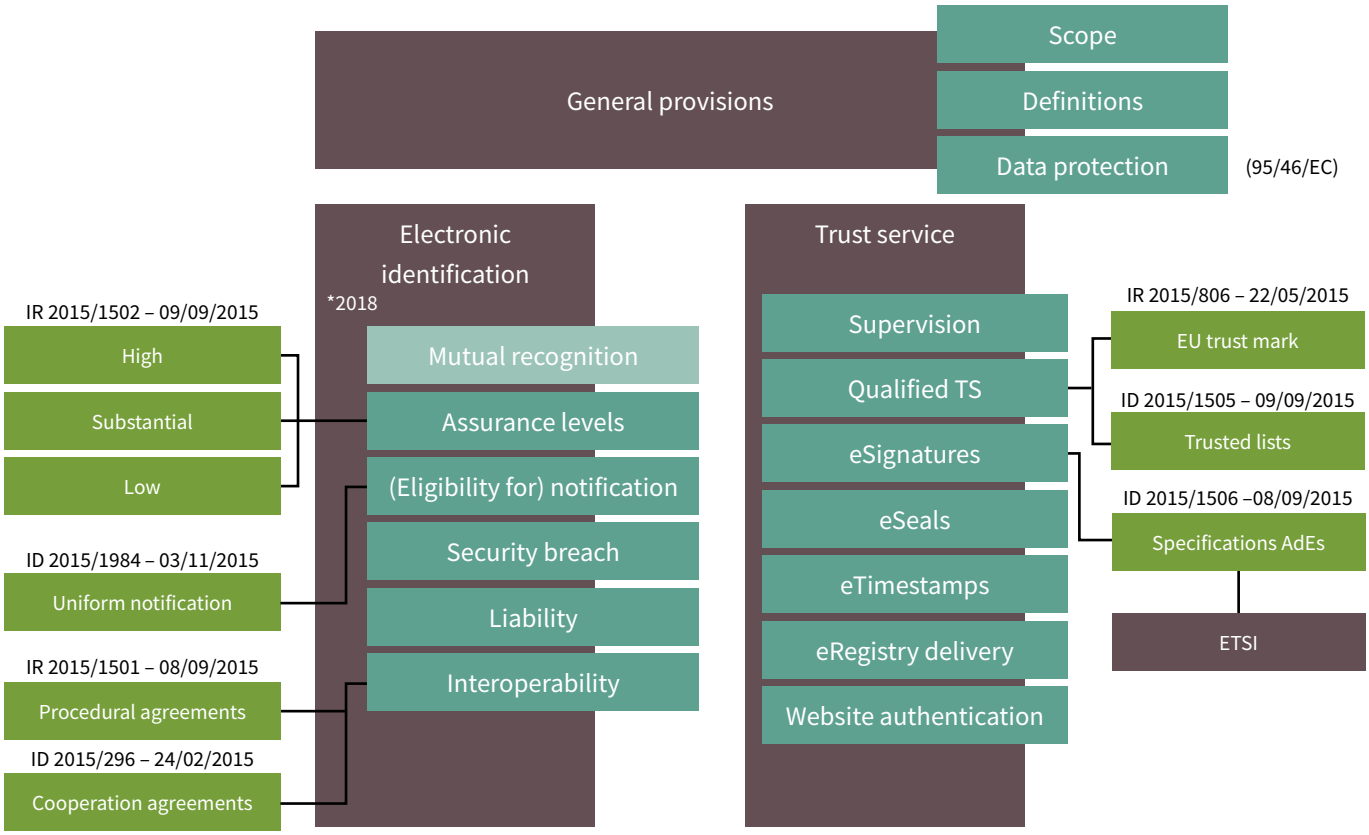

FIG 3: eIDAS overview

To support this new regulation, as well as the needs of the international community to provide trust and confidence in electronic transactions, the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI) have published a set of standards for Trust Service Providers (TSP), electronic signatures, electronic seals, and electronic timestamps. [5]

Mobile ID service providers in the EU will have to make decisions about how to acquire credentials, what type of authentication is needed, and how to provide a viable, secured, and easily deployable system. And, in order to truly take advantage of the secure, cross-border electronic transactions that eIDAS provides, a greater level of clarity in assurance levels is required.

6. Existing mobile ID implementations

Looking at implementations in the last ten or so years throughout Europe, the majority of existing mobile ID and authentication methods are based on PKI and SIM infrastructures. They tend to be implemented in countries where market penetration of mobile phones is high, such as Estonia, Austria, or Moldova.

Estonia

Estonia's mobile ID relies on the SIM-based approach because of a lack of NFC devices in the market to reach a significant percentage of the population. The key driver for this project was the desire to offer citizens speed, privacy, convenience and transparency for digital access to governmental services and information sources, including online applications and copies of official documents.

Estonia is seen as a pioneer of mobile ID technology, having launched its Mobiil-ID scheme as part of its wider ambition to become a leading digital economy in 2007. Estonia started rolling out eID cards in 2002, and since then its citizens have been using electronic identities and electronic signatures to engage with hundreds of public and private sector bodies. Since 2007, a mobile ID-compliant SIM-card, which is available from the nation's mobile phone operators, can additionally be used. The SIM card uses the same PKI as the eID card and the credential data is stored on a secured SIM card in the mobile handset. Private keys are stored on the SIM card along with a small application for authentication and signing. This technology has made it even easier for citizens to carry out a variety of activities, including voting over the Internet. In fact, in the 2015 Riigikogu elections, one-third of the Estonian electorate residing in a total of 116 countries used the Internet voting option to submit their vote. [6]

Austria

Austria has also been one of the leading countries for mobile ID adoption. In March 2004, Austria made its eID approach available on all media, including mobile phones, for the first time. In 2009, Austria deployed a server-based mobile ID solution through the European Commission's Project STORK. Cryptographic keys are kept on a central server securely stored in an HSM (high security module). The solution uses two-factor authentication involving the citizen's mobile device. For authentication, citizens use their mobile phone number plus a user-chosen password in a first step. In a second step, a one-time password is generated and transmitted to the mobile device to check that the mobile device is in possession of the authenticating citizen. The eID data are stored in the mobile ID system's database – not on the mobile phone – and can be accessed after successful authentication with the system.

The whole system is easy to use for citizens because no additional effort is needed, such as changing their existing SIM to an eID-enabled one – unlike the Estonian system. The government is keen to promote broad take-up. By April 2015, there were 500,000 active mobile ID users with 10,000-15,000 uses per day on a typical working day and 4,000-6,000 uses at the weekend. Today, Austrian citizens can choose whether to use a card or a mobile phone for their eID, with the latter being the most popular; in 2014, mobile ID activation was 15 times higher than traditional eID card activation.

Moldova

In Moldova, mobile ID is being delivered as part of the government's Governance eTransformation (GeT) project. The mobile signature service, which is based on the Mobile eID (MeID) infrastructure, was launched in September 2012 in partnership with Orange and Moldcell/TeliaSonera.

The system requires the regular mobile phone SIM card to be replaced with one that includes electronic ID functionality, similar to Estonia. The mobile ID solution allows citizens to confirm their identity and sign documents directly from their mobile phone by entering a unique user-selectable PIN code. Services that accept mobile digital signatures include eLicensing, tax declarations and criminal record requests. In addition, financial services companies and SMEs can take advantage of the nationwide infrastructure to provide their own eServices. [7]

Norway's BankID implementation

Although mobile ID schemes such as those deployed in Estonia, Austria or Moldova started life with a focus on enabling interaction with public services, citizens are now moving towards using them as a convenient gateway to a range of services, also beyond the government sector.

Large businesses such as payment processors, banks, transportation providers or eCommerce companies are venturing into the mobile payment and identification sectors with varying degrees of success.

For example, Norway's BankID speeds up financial and legal processes. There are currently two types of BankID: bank-stored BankID and mobile phone-stored BankID. Although the bank-stored BankID – where identity data is stored at the Norwegian Banks' Payment and Clearing Center (Nets) – is the most common one, there is growing interest in mobile BankID. In this scheme, the BankID and the corresponding identity data are stored on the SIM card of the user's mobile phone.

To access the BankID information on their mobile phone, citizens use their mobile phone number, date of birth, and a PIN code. BankID can be used for multiple online services. For instance, BankID can be used for an online shopping payment service called BankAxess; for Internet banking; to change address with the postal service; to place an offer on a property; for logging into municipal websites; and for purchasing units in equity funds. It can also be used for signing contracts, applying for loans, purchasing airline tickets, or filing tax returns.

In summary, it can be said that, while mobile ID implementations in the public sector have been successful, large-scale programs are still limited. The majority of EU member states have not yet made their government services accessible for citizens using mobile devices. Perhaps the complexity of bringing together the required security levels while ensuring ease-of-use is one of the reasons behind this slow development.

7. Vision and outlook

Infineon's and Silicon Trust's mobile ID vision is one of a modern, confident, secure and service-based relationship between governments / authorities and their citizens.

Mobile ID should enable governments to grant the consumer access to a wide range of online and offline services by using private mobile devices as a means of identification. Securely stored in a smart mobile device, the citizen's ID can be presented and verified with the highest level of privacy protection.

Accessing government services, such as citizen registration, change of address, and collecting benefits would be managed with mobile ID platforms, while at the same time, notification systems could be used by authorities to inform citizens quickly and cost-efficiently of upcoming deadlines or changes in policy.

For law enforcement, mobile ID can provide secured information on citizens on site which, in the case of accidents, crime scenes or liability scenarios can accelerate and, at the same time, de-escalate the retrieval of vital personal information.

In terms of security foundations, the secure element will continue to act as a trust anchor in mobile ID systems requiring high levels of security, such as financial transactions. This can be used for tamper-resistant credential storage and service processing. Choice of form factor – SIM card, embedded SE or microSD card – will be driven by the market needs of service providers and end users. The use of such trust anchors will ensure that mobile ID applications are implemented securely and fulfill specific privacy and security requirements, which deny disclosure of confidential credentials and allow the execution of applications in protected environments.

[1] https://technology.ihs.com/533599/nfc-enabled-handset-shipments-to-reach-three-quarters-of-a-billion-in-2015
[2] http://www.ey.com/Publication/vwLUAssets/EY-The-way-we-bank-now-A-world-of-change/$FILE/EY-and-BBA-The-way-we-bank-now-A-world-of-change.pdf
[3] http://www.globalplatform.org/specificationsdevice.asp
[4] https://www.gsmaintelligence.com/research/2015/03/the-mobile-economy-2015/491/
[5] https://www.enisa.europa.eu/topics/trust-services/guidelines/initiation_tsps
[6] Gemalto, Eric Billiaert, National mobile ID Schemes Whitepaper, Volume 1, 12/2014
[7] http://www.gemalto.com/brochures-site/download-site/Documents/tel-cs-mobile-id-moldova.pdf

Infineon Technologies AG

81726 Munich
Germany

Published by
Infineon Technologies AG

Order number: B181-I0444-V1-7600-EU-EC
Date: 03 / 2017

www.infineon.com