

## GOVERNMENT PROGRAMS



WHITE PAPER

# **National Mobile ID schemes Volume I**

Learning from today's best practices

December 2014

# Mobile ID – a universal and immediate bond

Looking ahead to 2020, many studies show the predominant role that mobile devices and - more broadly - connected objects, will have in our lives. The OECD reports that over 96% of the world population will be equipped with a cell phone by 2018 with over 7 billion cell phones in circulation. Mobility will be an essential factor for the agility and adaptability of the individual.

Some visionary countries have made the leap to **mobile identity or m-ID, meaning the creation of a mechanism - initiated using the eID component - for accessing online services with a high level of security thanks to mobile devices.** Electronic identity can be one of the bonds of trust between citizens and online public services, and in some countries banking services. This intuitive choice was founded on the hope of achieving better market penetration, better take-up by citizens and, as a corollary, a more optimum distribution of e-Government services.

The pioneers included countries where market penetration of cell phones and new technology is strong such as Austria, Estonia, Finland, Norway and Turkey. It was sometimes (Austria 2003) spurred by the need for a universal form of identification, sometimes (Estonia 2007) supplementing the national card program and accelerating the development of identity and electronic signature with the success that we know. Estonian President Toomas Hendrik Ilves recalled in Brussels on October 14, 2014 that the use of electronic signature in the country, has helped save the equivalent of one week of working time per person.



In 2014, Oman was the very first country in the middle east to complement its national electronic ID card with a mobile ID scheme.

Over the last few years mobile identity (mID) has seen growing uptake by citizens thanks to its ergonomics and high level of security.

The success and rapid uptake by citizens of **m-Government services** in all countries that have chosen to focus intensively on mobile communication devices to foster proximity and e-inclusion have demonstrated the strength of the bond of identification offered by mobile.

## Learning from past experience and today's best practices

We have learned from fifteen years of experience and practice that the greatest uptake of mobile identification will only be obtained if we keep the following principles in mind:

- > The principles governing the digital world are no different from those ruling the physical world.
- > The uptake of new uses is first and foremost about the value of the application. These hold true regardless of the tool in question.
- > Complexity should be masked. The governance organization for the identification system, its principal identities, secondary identities, authentication servers, the control and validation system and associated expertise should stay in the backstage where it belongs.
- > Technology and innovation will not motivate users. Communication on the extraordinary security effort

implemented and the legal validity of the system only generates mistrust. It spreads the idea that if there is still pride in the fact that the system is so different and unique, the system is still certainly immature. The presence of airbags and the best stopping distance have ceased to be factors in choosing a car. Cars have become comfortable, practical and functional everyday objects: this is their real purpose. Mobile internet too has become an everyday practice; it follows the same rules.

The 14 mobile ID schemes detailed in this document are part of the most ambitious ones and set a pattern that should be considered when creating and implementing a mobile identity infrastructure. Moreover, it is clear that the key components involve technology which is robust and certainly capable of delivering the results required.



## Public supervision is needed to coordinate approaches and experiences

Mobile identity is on the march. What remains is to adopt the new structure and codes that are needed to govern associated services and transactions.

In this context, the role of the public authorities is to:

- > Build and nurture a **national** momentum
- > Support and coordinate the **local** government investments through which local transformations, close to the community, can operate effectively and efficiently;
- > Make sure that these multiple local experiments create a **coherent and interoperable spectrum of solutions,**

because mobile citizens, going from one city to another, will need to find similar modes of services wherever they may be.

The dynamics of a digital framework of trust is then accelerated with mobile identity.

Evidence of uptake is confirmed and giving us clear signals of momentum in particular with the success of mobile online services.



# Usage and feedback from national experiences

The most advanced public initiatives in the field of m-ID are historically to be found in the following countries: Estonia, Austria, Finland, Turkey, Moldova and Azerbaijan. 2014 has seen acceleration in pilot programs or projects such as those in the United Arab Emirates, Oman, Iceland, Korea, India, Japan and Russia. Other large countries such as Brazil, Mexico, Italy and Spain are taking an interest.

In 2014, the most successful **private program** in the field of m-ID is without a doubt the PKI SIM-based Bank-ID program in Norway which brings together a very large number of service providers and mobile network operators.

Telenor had already been offering its subscribers the mobile Bank ID service for a number of years and in 2013 the other Norwegian MNOs started joining the service making it possible for their subscribers to have secure mobile authentication within the framework of the local BankID solution used in Norway for secure online identification and signature. The new mobile identity functionality works on all networks and all types of telephone and has already been adopted by more than 250 service providers in the country, including the major banks, as well as numerous other commercial organizations and government agencies. The arrival of mobile identity has doubled the average number of transactions per user to 12 transactions per month. According to the Bank ID website, 10% of the population is using mobile ID as of October 2014.

To help gain a better understanding of what is being done in the pioneering countries, we propose a rapid overview below of the approaches being adopted in eID and m-ID in the form of 14 country data sheets.

This panorama will give us a better understanding of the processes at work today and the trends that can be discerned. In each case, we will address the following aspects:

1. Governance: Who is at the head of affairs and what organization has been put in place?
2. Trust framework: What is the legal framework for the digital identity program?
3. State of eID program: What is the state of progress of the digital identity program?
4. State of mobile ID program: What is the state of progress with the national mobile ID program and what method of mobile authentication has been chosen?
5. Other comments relating to eID and/or m-ID
6. Leading applications of mobile ID and developments in process

Our journey will take us:

- > To Europe and the United States in order to understand the two cultures of trust and their models of identification
- > To the north and east of Europe to countries that have been the pioneers of m-ID for a number of years
- > To the Middle East, which has been boldly and determinedly treading the path of eGov 2.0 and digital trust since 2005, with strong technological competition between the GCC countries and also between SMART CITIES such as the sister cities of Dubai and Abu Dhabi
- > To Belgium and Austria, two pioneers of eID and modernization and who are preparing for eGovernment and SMART CITY convergence
- > To France and Germany, Europe's heavyweights, but also heavy structures to manoeuvre, albeit with numerous initiatives in France for its Smart City programs using NFC and m-payment structures.
- > Finally a diagonal sweep west then east - from Iceland to Turkey - with the latter putting a strong national spin on its leap into the future with mobility, a movement underway for the last 7 years.


# EUROPE – UNITED STATES:

## Two cultures of trust – two models of identification

Europe: a top-down model, where eGov 2.0 and SMART CITY converge and interoperate to advance towards the sustainable society set out in the Digital Agenda for Europe

- > Europe is characterized by the dominant faith in the sovereign state, seat of national trust and ultimate point of reference in terms of authority.
- > The prevailing model in national identification is based on the population or civil register (as the root) and either a unique ID (Belgium, Estonia), federated multiple IDs (Austria) or separated IDs (Portugal).

- > Fifteen years after the electronic signatures Directive 1999/93/EC, the eIDAS European Regulation voted in July 2014 sets up a framework of trust for electronic exchanges for 28 countries
- > Contactless and mobility have seen a rapid take-off since 2012, particularly through the adoption of NFC by many mobile operators and local authorities
- > We are seeing a true paradigm shift in eGov, moving to SMART CITY programs and local services


| <br><b>Europe (extended)</b>  | Governance  | Foundations of Trust framework   | State of eID program  | State of mobile ID program   | Comments  | Leading mobile applications   |
|--|---|--|---|--|---|---|
| <p>21 card-based eID programs in Europe (16 for EU28 in the strict sense)</p> <p>Turkish eID card about to be launched throughout the country (parliamentary decision in progress)</p> <p>Alternative of national digital identity/identification: Denmark (see data sheet) and the United Kingdom</p> | <p>European Commission DGCONNECT in Brussels</p> <p>CEN: European Committee for Standardization (Comité Européen de Normalisation)</p> <p>-----</p> <p>ETSI: European Telecommunications Standards Institute</p> <p>In the countries Generally coordinated by the Ministry of the Interior with the national population register at the core of the system when one exists</p> <p>Coordination of eGov schemes often falls under the responsibility of the prime minister and technical IT resources are often transverse</p> | <p>European Directive 1999/93/EC concerning electronic signature</p> <p>eIDAS regulation adopted in July 2014 on trusted electronic exchanges</p> <p>The regulation will give rise to more technical specifications for Member States (CEN)</p> <p>Vision - The Sustainable Society: Model of growth defined in the Digital Agenda for Europe 2020</p> | <p>150 million Europeans have an eID card, which corresponds to 30% of the population</p> <p>Sharp contrast in usage between countries</p> <p>Electronic signature used mainly by certain professions and applications</p> <p>1st launch in 1998 and 21st in 2014</p> <p>100M euros invested by the EC over the last 10 years in interoperability programs (STORK 1 and 2 programs)</p> | <p>The eIDAS Regulation, to the extent that it addresses electronic identification and signature, also applies to mobile ID.</p> <p>-----</p> <p>Currently different implementations with PKI SIM in the majority of cases.</p> <p>The most successful mobile ID programs worldwide are in Europe</p> <p>Many pilots in many cities Under SMART CITY programs in contactless mode coupling mobile ID and NFC</p> | <p>The eIDAS Regulation renders the 1999/93/EC directive null and void on July 1, 2016</p> <p>Technical proposal from German and French IT security agencies (BSI and ANSSI) for eIDAS tokens as of the summer of 2014</p> <p>Certainly an important building block as a legal framework for trusted exchanges both for Europe and with a view to a transatlantic partnership agreement on free trade</p> | <p>None in existence yet but the ingredients for success are in place as of 2014:</p> <p>eIDAS legal framework adopted, CEN technical framework currently in the process of being defined</p> <p>92% of the population in Europe has a mobile telephone as of the start of 2014</p> <p>NFC is getting strength after the announcement made by Apple in September 2014</p> |

USA: a bottom-up, liberal model where the strength of the commitment makes it binding.

- > **Faith in a model where individual freedom dominates the need for cohesion** and a stronger social bond. Model where the customs and the market eventually end up making the standard. The reliability of commitment of private operators is controlled by stringent laws but it is admitted that money ultimately covers the risk of prejudice due to accidental invasion of privacy or even fraudulent use of private data.
- > Though mobile identity is struggling to establish itself for want of a culture that embraces the sovereign

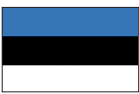
principle of identification (identity here is fundamentally declarative and the citizen does not lie given the heavy penalties for misrepresentation), **the principle of mobile trust is making inroads in mobile payments in the US:**

- The SUBWAY restaurant chain is embarking in late 2014 on the largest NFC deployment in the country, with NFC payment terminals by Softcard (a joint venture between AT&T, T-mobile and Verizon) across 26,000 service points
- Apple is launching its payment application Apple Pay promoted as a Killer App with the iPhone 6
- San Francisco is rolling out a city-wide extension of its NFC PayByPhone parking system.



| <br>USA  | Governance   | Foundations of Trust framework  | State of eID program   | State of mobile ID program   | Comments  | Leading mobile applications   |
|---|--|---|--|--|---|---|
| <p>No national identity card</p> <p>No national digital identity program</p> <p>But driver's license serves de facto as an identity card</p> <p>Digital identity cards issued by the State for its personnel</p> <p>No national population register</p> | <p>The White House</p> <p>Department of Homeland Security</p> <p>Department of Commerce</p> <p>-----</p> <p>Standardization body:</p> <p>The National Institute of Standards and Technology (NIST)</p> <p>Department of Commerce</p> <p>-----</p> <p>Various initiatives taken in particular by the DMV (Department of Motor Vehicles) With a view to studying a mobile-based driver's license (Georgia and Florida)</p> | <p>Homeland Security Presidential Directive 12 (HSPD-12) dated August 27, 2004 (HSPD-12) defines a policy for a common identification standard for Federal employees and contractors. Smart cards arrive on the scene as of 2007: Personal Identity Verification (PIV) cards</p> <p>Presidential initiative in 2011: NSTIC (National Strategy for Trusted Identities in Cyberspace) supervision of the Department of Commerce</p> | <p>DoD (Department of Defense) cards for military personnel in place since 2001 (cryptography, PKI)</p> <p>Electronic identification and authentication by contact-based PIV smart card for many government administrations</p> <p>Pilot projects financed by the NIST in September 2014 to implement a reliable system for digital identification as part of the NSTIC initiative</p> | <p>No centralized mobile ID project</p> <p>In March 2014, the NSTIC published a guide to derived mobile identity making it possible, within certain limitations, to use derived identity credentials on mobile from PIV cards.</p> <p>Very recent projects on derived identity credentials on Mobile within the framework of the DoD's CAC and driver's licenses</p> | <p>The question of national ID is not just about digital ID. There is no official Federal document. Very fragmented situation with regard to birth certificates (14,000 different formats) and driver's licenses: a de facto form of ID</p> <p>34 states require a form of ID to vote, such as an invoice, social security number, etc.</p> <p>Cases of massive data theft which were again on the rise in 2014 pushing large companies like Google, Amazon and Apple to move towards simple OTP solutions (Apple iCloud)</p> | <p>Not yet in place</p> <p>But numerous solutions in the private sector use mobile telephones for two-factor authentication</p> |

## The pioneers of mobile ID

**Estonia:** banked on mobility as early as 2007 to boost eID usage


| <br>Estonia  | Governance  | Foundations of Trust framework  | State of eID program   | State of mobile ID program  | Comments   | Leading mobile applications  |
|---|---|---|--|---|--|--|
| <p>National program</p> <p>eID and mobile ID are part of daily life since 2005 and 2007.</p> <p>Level of maturity of use: Very high thanks in particular to education and communication</p> <p>Estonia is proving to be a source of inspiration to its neighbors and is cooperating with Lithuania, Latvia, Denmark and Finland</p> | <p>Involvement of the Public Authority at the highest level to coordinate deployment across public and private entities.</p> <p>Technical Management of the Program by the Ministry of Economic Affairs and Communications</p> <p>Choice of a single Certification Authority SK (AS Sertifitseerimiskeskus), Linked by a Public-Private Partnership. The Authority was created by four companies from the world of banking and telecoms: EMT, Hansapank, Eesti Ühispank and Eesti Telefon</p> | <p>European Directive 1999/93/EC and the subsequent Estonian law concerning electronic signature adopted on December 15, 2000</p> <p>agreement for recognition of qualified signature with Finland, Belgium, Portugal and Lithuania for the creation of companies</p> <p>Law prohibiting the government from requesting data that it already has in its possession</p> <p>Introduction of criminal sentences for cyberattacks</p> | <p>Electronic identification and authentication by contact-based national identity smart cards as of 2005.</p> <p>100% of the population has this card.</p> <p>eID and its three functions secured by a national PKI network: identification, authentication and qualified electronic signature (with same validity as written signature)</p> <p>Heavy promotion of the model at international level</p> | <p>Since 2007, mobile identity on SIM card can be activated online by means of a specific application which uses the electronic identity card as a means of identification.</p> <p>Then by acquiring a special SIM card from mobile operators. Certificates are valid for 3 years</p> <p>Electronic signature and mobile authentication by PKI SIM.</p> | <p>The technology for mobile ID is the same as that for eID and applications which require a high level of security such as e-voting are available immediately.</p> <p>The rapid modernization of government administrations and the private sector in Estonia has clearly demonstrated the benefits of a secure and multimodal sovereign digital identity. Mobile ID is accepted by 90% of online services available in the country in September 2014</p> | <p>More than 300 private and public organizations use mobile ID</p> <p>e-Banking is the flagship application</p> <p>Numerous applications for students &amp; universities</p> <p>The GoSwift application for reserving one's place to cross borders won the 2013 prize for innovation. It dematerializes the queue by creating a virtual queue. An application developed at the request of the Ministry of the Interior.</p> |

**Moldova:** bypassing eID to shift straight to mobile ID


| <br>Moldova  | Governance  | Foundations of Trust framework   | State of eID program                 | State of mobile ID program  | Comments  | Leading mobile applications   |
|---|---|--|--------------------------------------|---|---|---|
| <p>No card-based national digital identity program</p> <p>Mobile ID program with electronic signature service since the end of 2012</p> | <p>Coordinated by the eGovernment Center created in August 2010, responsible for implementing the country's eGov Agenda</p> <p>Active communication with users</p> <p>Certification authority CTS</p> <p>Agreement between the two operators Moldcell, Orange, the CA and the authorities</p> <p>The Government is financing the certificates</p> | <p>Electronic signature adopted in Moldova on July 15, 2004.</p> <p>On May 29, 2014, the new law on electronic signature is adapted to bring it into line with Directive 1999/93/EC</p> <p>Applicable on January 4, 2015 pending eIDAS</p> | <p>No eID national identity card</p> | <p>Launched since the end of 2012</p> <p>The process of registering with the operator takes 15 minutes</p> <p>Strong authentication and <b>PKI SIM</b> electronic signature service; secret with PIN code</p> <p>The MNOs have invested in their systems and users pay for the service.</p> | <p>Mainly used by companies in B to G</p> <p>International recognition with the GSMA Mobile Award in 2013</p>  | <p>96 e-services available</p> <p>23% of social security forms approved with mobile ID as of 2013</p> |



**Finland:** The creation of the circle of trust bringing together the MNOs, the private and the public sectors enabling interoperability with the three mobile ID services and the seamless use of the mobile ID service for all users is something unique in the Finnish Mobile ID model. It will be adopted also in the soon to be revised legislation on strong electronic authentication services.


| <br>Finland  | Governance  | Foundations of Trust framework  | State of eID program  | State of mobile ID program  | Comments  | Leading mobile applications   |
|---|---|---|---|---|---|---|
| <p>National program</p> <p>eID card launched in 1999, electronic certificate on all cards. Card updated in 2003 to support electronic signature.</p> <p>Health insurance information added on the card upon request.</p> <p>The interoperable mobile ID service developed by the three national operators was launched in Nov 2010.</p> | <p>Initiative coordinated by the national population register center (VRK) in association with the Ministry of the Interior</p> <p>VRK is no longer responsible for the issuing of electronic certificates for Mobile ID but issues a unique identification number (SATU) to citizen or resident.</p> <p>The mobile ID working group members include the three MNOs and FiCom (Finnish Federation for Communications and Teleinformatics)</p> | <p>European Directive 1999/93/EC and the subsequent Finnish law concerning electronic signature adopted in 2003</p> <p>Modification of the law in 2009 to take account of mobile signature and make it legal for the signature of contracts, agreements, etc.</p> | <p>Unit cost of eID card: €53, Not mandatory. 10% of the population has one. The health insurance card Kela can also be incorporated into the ID card.</p> <p>Electronic identification and authentication by contact-based national identity smart cards.</p> <p>Very low level of use online. The private BankID, Tupas system is in fact the country's official authentication system.</p> | <p>The creation of national mobile ID standard supported by the three operators in 2010 allowed rapid progress to be made with services.</p> <p>Acquisition of a special PKI SIM card from mobile operators at a face-to-face meeting, or pre-registration online via Tupas</p> | <p>Before: For nearly 10 years, the method of authentication in Finland, for the banks, business and eGov, was an OTP on a paper list + PIN code, which is a legal form of authentication. (The BankID system)</p> <p>Today: mobile ID with PKI SIM as the method of authentication is making rapid progress. 50,000 regular mobile ID users in 2014. mobile ID is free for users and paid for by the providers of online services.</p> | <p>Over 300 public and private services accepting mobile ID.</p> <p>Most popular services are: Getting involved with citizens' initiatives Working with Insurance services Checking one's medical prescription Applying for benefits Opening a gaming account Reporting an offence to the police Accessing health services</p> <p>source <a href="http://www.mobiilivarmenne.fi/en/">www.mobiilivarmenne.fi/en/</a></p> |

**Denmark:** an atypical model of trust secured simply using a login and password


| <br>Denmark | Governance   | Foundations of Trust framework  | State of eID program  | State of mobile ID program   | Comments  | Leading mobile applications   |
|--|--|---|---|--|---|---|
| <p>National digital identity program since 2007</p> <p>No physical identity card</p>           | <p>Nem-ID program coordinated by the Ministry of Finance</p> <p>Cooperation between banks and government</p> <p>Managed by a private company Bank + public sector. Steering by (STS) ministries, regions and municipalities for the country's eGov strategy.</p> | <p>Law on communication by e-mail with government authorities (mandatory in 2015 – no more paper letters)</p> | <p>Nem-ID: requested online with unique citizen number + passport or driver's license number. Cross-checked by police and issuing of a login/password and a list of passwords on paper.</p> <p><b>Simple OTP</b><br/>Easy to use and popular: 90% of citizens 99% of businesses</p> | <p>No specific mobile ID in the same way as in Finland or Estonia.</p> <p>Nem-ID can be used on mobile as only a simple login and password is required</p> | <p>National DDoS attack on April 11, 2013 blocking the banking system</p> <p>Browser security middleware rewritten in July 2014 in java</p> <p>Considering move towards other authentication factors (biometrics, etc.)</p> | <p>Single point of entry to services: Portal for citizens, businesses and healthcare</p> <p>eGov applications have to be extensively adapted to mobile mode</p> |

# Middle East: daring to tread the road of eGov 2.0 and digital trust since 2005

**United Arab Emirates:** in the technological vanguard, and not waiting around for Europe


| <br>UAE  | Governance  | Foundations of Trust framework  | State of eID program   | State of mobile ID program   | Comments   | Leading mobile applications                                      |
|---|---|---|--|--|--|--|
| <p>National program</p> <p>eID: Pilot phase in 2005 and national launch in 2007 the project combines registration of the population and issuing of the card</p> <p>mobile ID: pilot phase in 2014</p> | <p>The program to modernize the sovereign identity system has been entrusted to an independent public authority, <b>the EIDA (Emirates Identity Authority)</b> responsible for implementation of all phases of the program. The core of the system is the national population register</p> <p>Infrastructure that is interoperable for all ministries and government administrations, and is open to the private sector</p> | <p>Created in 2004 by decree No. 2 of the independent authority EIDA responsible for the national register and the distribution of eID cards</p> <p>Federal Law No. 1 of February 2006 concerning Electronic Transactions and Commerce (electronic signature)</p> | <p>Nearly 95% of the population is registered and 80% are holders of the eID card. The biometric card is issued to Emiratis and residents who account for the majority of the population (80%). The card is a contact AND contactless card</p> <p>Electronic identification and authentication by contact-based national identity smart cards.</p> <p>EIDA manages a PKI public key infrastructure</p> | <p>As part of a project announced in May 2013, mobile ID is being tested in 2014 with a pilot involving PKI SIM cards (with operators) with face-to-face identification.</p> | <p>The first mobile apps appeared at the end of 2013 with support for geolocation in particular. These are applications redesigned for smart phones as part of the Smart eGovernment project.</p> <p>Project at a very advanced stage to make the eID card work as a payment and withdrawal card 500,000 readers handed out in 2013 to encourage use</p> | <p>No major deployment yet</p> <p>Generalization in progress</p> |

**Qatar:** looking to move quickly and integrate citizens and residents


| <br>Qatar   | Governance  | Foundations of Trust framework   | State of eID program   | State of mobile ID program   | Comments  | Leading mobile applications                     |
|--|---|--|--|--|---|---|
| <p>National program</p> <p>eID was launched in 2005</p> <p>Next steps may include extending the program with the use of mobile PKI where citizens log on to the Hukoomi portal using either their eID or mobile phone.</p> | <p>The eID program is managed by the Ministry of the Interior.</p> <p>Information technology, and in particular aspects concerning identification, authentication and signature, is managed by the Ministry of Information and Communications Technology (ictQatar) for all ministries.</p> | <p>Decree Law No. 36 of 2004 establishing ictQatar Ministry of information and communication technologies</p> <p>Law of August 19, 2010 on Electronic Commerce and electronic signature in particular.</p> | <p>90% of Qataris and residents have the biometric card</p> <p>Electronic identification and authentication by contact-based/ PKI national identity smart cards. 500 services on the country's eGov network by ictQatar offering Single Sign On and Electronic Signature since February 2014</p> | <p>The PKI infrastructure and certificate authority put in place in 2007.</p> <p>It may be hosting the mobile ID pilot program in a few months time.</p> | <p>mobile ID will enable authentication and signature of applications eGov available on the country's federated portal.</p> | <p>Not yet in place, still in project phase</p> |

## How two pioneers of eID and eGovernment are facing up to m-ID

### Belgium: eID on road to sustainable society and Smart Cities


| <br>Belgium                                      | Governance  | Foundations of Trust framework  | State of eID program   | State of mobile ID program  | Comments   | Leading mobile applications  |
|---|---|---|--|---|--|--|
| <p>National eID program</p> <p>Launched in 2004</p> <p>mobile ID program: technical solutions studied and in validation phase</p> | <p>Coordinated by the <b>Ministry of the Interior</b></p> <p>Main parties involved</p> <p><b>National population register</b> (Ministry of the Interior)</p> <p><b>FEDICT</b> (FEDERAL PUBLIC SERVICE, INTERIOR)</p> <p>Transverse body providing technical IT resources for the deployment of the interoperability infrastructure</p> <p>A Public Trusted Third parties Organization to protect data flows</p> <p>Five personal data protection organizations at the core of the technical system deployed</p> | <p>European Directive 1999/93/EC and the subsequent Belgian law adopted on October 20, 2000.</p> <p>Royal Decree on eID in 2004 and law on access to personal data 2012 : Fedict responsible, for security and respect of privacy in exchanges of personal data and electronic cooperation between services.</p> <p>Law on the non-duplication of administrative information requests in 2014</p> | <p>10 million contact-based cards in circulation (100% of the target population)</p> <p>30% of cards activated for use for online identification.</p> <p>More than 700 applications use eID</p> <p>Electronic identification, authentication and signature by contact-based national identity smart cards.</p> <p>Signature widely used in the professional sphere</p> | <p>Program ready but pending decision by new government formed in September. 2014</p> | <p>eID program is founded on excellent regional cooperation, extending the scale of the success by investing in all local services.</p> <p>«Marketing» approach with in-depth consideration given to the product and its presentation, acceptability and promotion (communications)</p> <p>Notion of role allowing for use in the professional sphere</p> <p>Health card merged with the eID card in 2014.</p> | <p>mobile ID not yet in place</p> <p>But ambitious NFC mobile payment program <b>very well disseminated since 2012</b></p> <p><b>SMART CITY</b> at the forefront</p> <p>A European first: European Bank investing 400 million euros to support <b>«Smart Cities &amp; Sustainable Development»</b> in all Cities</p> |

### Austria, a pioneer of eID and paperless government, launched mobile ID as early as 2004


| <br>Austria  | Governance  | Foundations of Trust framework   | State of eID program   | State of mobile ID program   | Comments  | Leading mobile applications  |
|---|---|--|--|--|---|--|
| <p>eID available since March 2004 on all media including cell phones</p> <p>New mobile ID since 2009</p> <p>The citizen can choose the medium used to store their eID: either on card or mobile. <b>MODEL IS THE ONLY ONE OF ITS KIND IN EUROPE</b></p> | <p>Chancellery</p> <p>eGovernment Innovation Center with the technical support of the University of Graz</p> <p>National population register (citizens and residents)</p> <p>Center for online security</p> | <p>European Directive 1999/93/EC and Austrian law of December 2001</p> <p>Law of March 2004 for eGov program</p> | <p>Digital identities derived from National Register per domain (Liberty Alliance model). The citizen's electronic card can be used for identification and authentication (signature and mandate). Physical medium can be a bank card, health card, student card, signature card, service card or mobile telephone</p> | <p>eID and Signature on mobile since 2009 developed within STORK project</p> <p>In 2014: 300,000 signatures a month and 20 to 25,000 new mIDs/month</p> <p>Authentication uses the mobile phone number + password + OTP code. The eID is stored in the mobile ID system's database - not in the phone - and accessed after successful authentication with the system. SMS channel, no cryptography</p> | <p>In 2012, all the developments for ID, signature and the signature server were made available online as open source</p> <p>Close synergy with the cities of Vienna, Graz, Salzburg and Linz</p> <p>Austria No. 1 in eGov in the EU28-Benchmark reports for last seven years</p> | <p>More than 200 applications use the federated identity for businesses and citizens</p> <p>Job search with eJob room</p> <p>Online services for breeders</p> <p><b>SMART CITY</b> Lots of innovative applications at city level</p> <p><b>VIENNA</b> in Top 10 of <b>SMART CITIES</b></p> <p><b>KLAGENFURTH</b> NFC City - a genuine mobile library</p> <p>Generalization of Mobile payment in progress</p> |

## The European heavyweights, hard to steer, some remarkable success stories

**France:** lagging behind on eID- booming with Smart City, and mobile payment projects with NFC


| <br>France   | Governance  | Foundations of Trust framework   | State of eID program  | State of mobile ID program  | Comments   | Leading mobile applications  |
|---|---|--|---|---|--|--|
| <p>No sovereign national digital identity program (either for eID or mobile ID)</p> <p>Numerous semi-public and private initiatives such microchip-based service smart cards for many public organizations</p> <p>France connect national scheme announced as a state driven facebook connect (digital ID federation)</p> | <p>The French National Agency for Secure Documents (Agence Nationale des Titres Sécurisés - ANTS) created in 2007 – body under the supervision of the Ministry of the Interior</p> <p>Ministry of Industry and the Digital Economy</p> <p>The CNIL (National Commission on Information Technology and Civil Liberties)</p> <p>Standardization body dependent on the prime minister French national agency for the security of information systems (ANSSI)</p> | <p>European Directive 1999/93/EC and the subsequent French law concerning electronic signature adopted in March 2000</p> <p>The French Data Protection Act of 1978 («Loi Informatique et Liberté de 1978»)</p> <p>Law on eID in 2012. The Constitutional Council has limited the scope of the card. Project not launched; not currently on the agenda (Sept. 2014)</p> | <p>The federated portal «mon service publique» («My public service) provides a single <b>login/password</b> for several government and healthcare/social security services. . The payment of VAT is secured by <b>PKI token</b>. Various initiatives in the banking sector based on <b>OTP</b>...</p> <p>France Connect announced in Sept 2014 will be a public service like facebook connect and will federate public identities for the second half of 2015</p> | <p>No national mobile ID program</p> <p>No private m-ID offer from operators at this time</p> <p>France Connect announced in Sept 2014 will be in pilot phase in 2015. It will act as a proxy and will not be an ID provider.</p> | <p>No national population register</p> <p>Multiple identification credentials for a single citizen</p> <p>The French post office «La Poste» provides a digital identity in the form of a <b>login/password</b> after a face-to-face registration</p> <p>The INES eID card project from 2005 has not come to fruition<br/>The IDéNum project from 2010 has not come to fruition</p> | <p>eGov 2.0 blends with the numerous SMART CITY programs</p> <p>CITIZY consortium created by the Operators and Public Authorities to develop a deployment of Mobility-oriented local programs with use of NFC for identification and payment</p> |

**Germany:** an eID infrastructure in place but austere, mobility conquers payment


| <br>Germany  | Governance   | Foundations of Trust framework  | State of eID program  | State of mobile ID program  | Comments  | Leading mobile applications   |
|---|--|---|---|---|---|---|
| <p>National eID program launched in Nov 2010</p> <p>Credit card format contactless smart card with identification but no signature capabilities yet</p> <p>No national mobile ID project proposed either by the government or operators</p> <p>-----</p> <p>electronic signature available since 2000 by token or OTP</p> | <p>Coordinated by the <b>Ministry of the Interior</b> for the card component</p> <p>But no promotion of services</p> <p>Standardization body: BSI</p> <p>The Fraunhofer national institute for public research conducted the pilot scheme provided technical support for startup</p> <p>Cards are issued by the country's 3,200 <b>municipalities</b></p> <p>-----</p> <p>In the private sector, Trust Centers issue signature certificates. Used by professionals</p> | <p>European Directive 1999/93/EC and the subsequent German law concerning electronic signature</p> <p>Legal amendments in 2012 and 2013 for online identification; signature with the new identity card and the electronic residency permit as an electronic equivalent of the physical form only came into effect in 2013.</p> | <p>More than 30M eID and residents cards in circulation in 2014.</p> <p>30% of cards activated for use for online identification.</p> <p>Electronic identification and authentication by contactless national identity smart cards Six-figure PIN code</p> <p>eID not promoted by municipal authorities</p> <p>Difficulty of training over 136,000 people</p> | <p>Possibility considered of deriving a digital identity from the contactless card by reading with an NFC telephone.</p> <p>Project abandoned mid-2013 due to lack of public and private financing for development</p> <p>No offer in Germany at this time (September 2014)</p> | <p>Digital identity and biometric option <b>free-of-charge upon request submitted to the municipal authorities</b></p> <p>modification of PIN code upon request</p> <p>1 M readers handed out free-of-charge</p> <p>Hundreds of public and private services used the eID card online</p> <p>Google, eBay Amazon, Facebook...not interested</p> <p>The card does not always have signature capabilities at this time</p> | <p>No national project in 2014</p> <p>and not yet on the agenda (September 2014)</p> <p>In Germany, MasterCard working with Deutsche Telekom, Telefónica Deutschland, Vodafone to create a <b>new mobile platform</b> and to accelerate development of mobile payment in the country.</p> |

# From east to west, Smart cities, eID, and NFC pave the way for sustainable European society

**Iceland:** firmly committed to the sustainable society

| <br>Iceland  | Governance   | Foundations of Trust framework                                 | State of eID program  | State of mobile ID program  | Comments  | Leading mobile applications  |
|---|--|--|---|---|---|--|
| <p>National digital identity program since 2008</p> <p>mobile ID program launched in 2014</p> | <p>Project coordinated by the Ministry of Finance and Economic Affairs and financed by the banks.</p> <p>1 national CA: Audenni responsible for technical aspects of project, itself under the responsibility of the Ministry of Finance</p> | <p>Law on electronic signatures adopted in Iceland in 2001</p> | <p>Certificate available on credit cards</p> <p>NO national identity card</p> <p>National PKI Infrastructure since 2008</p> <p>Little use by citizens between 2008 and 2013</p> | <p>National launch of mobile ID in 2014 financed by the banks</p> <p>On the same PKI network deployed in 2008 (PKI SIM)</p> | <p>eID on bank cards was not a great success</p> <p>PKI network compliant with international standards.</p> <p>Desire not to have to opt for custom solution.</p> <p>Sharing of best practices with involvement in the European STORK project</p> | <p>Banking applications are now available and using Mobile ID to authenticate and validate transaction with digital signature. eGov applications are also in service, and government department are using mobile ID for its own purpose.</p> <p>Reykjavik at the forefront of the SMART CITY trend<br/>For a Sustainable Iceland</p> |

**Turkey:** the south-eastern pioneer of mobile ID, opted for the mobility route from the outset in 2007

| <br>Turkey   | Governance   | Foundations of Trust framework   | State of eID program   | State of mobile ID program   | Comments   | Leading mobile applications  |
|---|--|--|--|--|--|--|
| <p>National eID card project initiated since 2010 with full-scale pilot conducted.</p> <p>Mobile ID Turkcell 1<sup>st</sup> generation Then 2<sup>nd</sup> gen with Turkcell, with Cloud-ID Project for 2015-2016</p> | <p>Very strong willingness at political level Coordinated by the Ministry of the Interior Main parties involved</p> <p>General Directorate of Population and Citizenship Affairs</p> <p>Partnership with public research body Tübitak which defined the technical environment [cryptography, key management, etc.] Coordination of industry and suppliers with national test laboratory placed at their disposal</p> | <p>Electronic Signature Law 5070 of January 2004</p> <p>Law on eID set to be adopted at the end of 2014</p> <p>Adapted banking practices and law on financial crimes</p> | <p>Pilot carried out successfully in the city of BURSA. Project ready for national launch. Project on standby since August 2014. Parliamentary decision expected at the end of 2014</p> <p>Signature widely used by professionals on the PKI network</p> | <p>Started to deploy an mobile ID solution in 2007 (electronic signature by mobile telephone), based on PKI with the operator Turkcell</p> <p>-----</p> <p>First generation with applet on SIM and SMS and second generation based adaptable Secure Element in the Cloud - Tests in 2015. Proof of concept planned for 3Q 2015</p> | <p>For the launch of eID: close coordination with central and local authorities, and post offices, with Integration with banks (ATM, eSignature) Garanti Bank shall place certificates on the national eID card.</p> <p>eID will act as the key for access to Turkey's eGov portal</p> | <p>Main uses in the world of banking due to the initial support of main banks</p> <p>Identification on eGovernment portal with mobile ID</p> |

# Conclusion

These nationwide mobile ID schemes are part of the most ambitious ones and set a pattern that should be considered when creating implementing a mobile identity infrastructure.

The experiences in pioneer countries show a surprising degree of convergence:

## In terms of the objective of the eID and mobile ID programs

The objective is to foster and to drive the digital modernization of social bonds with trusted identities, for a new era of prosperity known as "sustainable society". All programs converge and express an awareness on the part of a majority of public authorities to take action to:

- > Make our society more cohesive, more human, more local and more connected,
- > Adapt to the new situation where mobility is becoming the standard for connectivity,
- > Take on board the need for meaning, ease and agility that must govern all exchanges of information between people, between people and urban connected objects, between people and the information resources that make up the wealth of modern digital society.

The countries that are now moving forward are in fact so many laboratories, all developing standards, patterns of growth and technological development, practice and policy.

The name of the game is therefore:

- > By establishing the sustainable digital society to strengthen and renew social bonds, through **SMART CITIES programs** which make it their emblem,
- > Through the understanding that **with mobility becoming the norm, these social bonds from now on will "go through" those mobile devices with which it is expected that 96% of the world's population** will be equipped within 5 years.
- > Active and effective collaboration between public authorities, operators, banking and financial institutions and manufacturers, to establish a highly secure standard for mobile environment and a universal approach to build in and guarantee this security in close-up **contactless** information exchanges through **NFC technology in particular**, thereby opening communications to the world of the Internet of Things.



Reflecting on and redefining the future therefore equates to considering smart cities as the broad frame of reference, where the vast majority of the interactions of the modern connected world are played out.

## In terms of the governance framework

Our journey shows that development is the fastest, the most productive in bringing effective progress and most secure where strong leadership is exercised by the public authority.

This creates a framework for collective confidence, which local authorities and stakeholders in public and private services can use to deploy their offerings and propose all manner of exchanges conducive to creating value. These in turn can be beneficial for the prosperity of society as a whole. The overall dynamic fosters adoption by the greatest number of citizens or users.

Creating this environment is also known to take time as experienced by all pioneers. The political will to take action can then be a catalyst for a faster set up.

## In terms of the legal framework of trust and the sovereign source of identity

Although it does not appear in our travel log, it is important to remember the source of the legal certainty or security that underpins the reliability of any form of identification in general, and digital in particular, in most of the countries along our journey, and, paradoxically, also in the United States.

The personal identity of a person, from a legal point of view, resides in the vast majority of countries in the civil registry and is hence guaranteed by the State. Although control of this identity in countries like the United Kingdom or the United States may be purely declarative, it essentially consists of a set of factual and legal data relating to an individual (date and place of birth, full name, affiliation, etc.) that has been legally recognized, witnessed or certified, and which allows the individual to be identified uniquely.

The function, constituting the parent repository for any identification data, is typically sovereign and protected. The major efforts to secure this function, observed in all countries in recent years, are testimony to a new awareness of its fundamental value and its potential role in the protection of the social bond.

This is why even in countries where identity cards are not customary, we see a trend to looking for ways to create a **reference point for identity** that can then be transposed into the digital world where there is a need for a way of guaranteeing the identity of the parties to a transaction or exchange.

## In terms of citizen uptake

Our journey has shown strong support for translation of eID and eGovernment programs to the mobile world, as if the privacy and personal control of exchanges were better on mobile devices by virtue of the fact that we carry them with us everywhere, about our person.



This is sociologically interesting and it has to be considered to be a confidence factor parameter to be included in the solutions. We have probably reached a maturity threshold comparable to the use of the smart chip credit card. Experience of protection in the event of an incident has created a very high level of confidence.

The popularity of the mobile channel and contactless services through NFC is now a reality.

## In terms of technological approach

90% of the technical authentication methods in these projects are based on PKI and SIM infrastructures. NFC technology is envisaged as of 2013 to derive sovereign identity credentials and under test in several countries in 2014.

This ID derivation trend seems to be confirmed even in the United States: As of March 2014, the American standardization body, the NIST (National Institute of Standards and Technology – Department of Commerce) has issued recommendations for deriving mobile identity credentials from Federal PIV cards (Guidelines for Derived Personal Identity Verification Credentials).

This goal is to create a mobile identity (mobile ID) that provides access to online services securely. The creation of this mobile identity is a technical extension - aka derived credentials - of the eID card. It provides the same high level of authentication.

Mobile identity would appear to be on the march and set to become a new norm. What remains is adopt - fundamentally and permanently - the structure and codes that are to govern mobile services and the world of transacting in mobility. It is also time to get ready to massively educate citizens to prepare for the future, for the expected success and growth.



Public supervision is needed to coordinate approaches and experiences. In this context, the role of the public authorities is to:

- Build and nurture a national momentum
- Support and coordinate the local government investments through which local transformations, close to the community, can operate effectively and efficiently
- Make sure that these multiple local experiments create a coherent and interoperable spectrum of solutions, because mobile citizens, going from one city to another, will need to find similar modes of services wherever they may be.

Evidence of uptake is multiplying and giving us clear signals that have been awaited for some fifteen years. **The future is being decided now** and the sustainable society of 2020 is everywhere within striking distance, just one bold Mobile eGovernment or Smart City program away. Ultimately, these programs share a common mission: to bring people closer together, connect them, boost their communication and exchanges, and why not to nourish the hope of better life.

**2020 is today.**

Notes:

A series of 18 horizontal dotted lines for writing notes.

## About Gemalto

Gemalto is the world leader in digital security with 2013 revenues of €2.4 billion. In the public sector, Gemalto provides secure documents, robust identity solutions and services for governments, national printers and integrators in the service of citizens. Its products and solutions are deployed in more than 80 government programs worldwide.

Gemalto is contributing to more than 25 ePassport initiatives and to 27 national eID programs. Leveraging on its Valimo Wireless activities, Gemalto is the leading solution provider for mobile user authentication and digital signatures with over **20 ongoing mobile Identity projects** and enabling millions of mobile users to start accessing government services with enhanced security. Among those projects, 8 are used specifically in national eID schemes to secure the access to eGovernment services.

Our contribution to these projects provides us with an excellent overview of the technology involved, its applications and the quality of information systems, as well as the social context of its use. Gemalto also collaborates with its clients to report and share best practices from around the world. This is the purpose of the present white paper.

This white paper presents the experiences of 14 advanced countries in terms of eID and mobile ID and models of partnership with banks and operators. Its goal is to give all public stakeholders and their partners the understanding, insight and tools to include mobile services and Mobile Identity as defining features of their modernization process for the years to come.

We hope it will give you the courage and desire to join forces with those at the forefront of pioneering the sustainable society of tomorrow.