Worldbank's Secure eID Toolkit for Africa

Marc Sel – Tomas Clemente Sanchez

PricewaterhouseCoopers Enterprise Advisory

marc.sel | tomas.clemente.sanchez@pwc.be

Abstract

This article provides a high-level functional and technical overview of the Worldbank's Toolkit project 'Secure Electronic Identity for Africa'. The Toolkit project was initiated by the Worldbank in 2012, with sponsorship of the French government. Its aim is to provide African nations with a guidebook addressing all required elements to establish a secure electronic identity system in their country. The Toolkit is expected to be publicly announced in 2013. Implementation funding is to be provided through a PPP (Public Private Partnership) including participation from the Worldbank.

The Toolkit proposes a mixed ecosystem of government and private sector operators such as MNOs (Mobile Network Operators). It combines elements such as the potential collaboration of government entities such as a National Identity Register, other registers such as an Election Committee Register and Registers of Births and Deaths, various private Trust Service Providers, and a combination of mobile (e.g. SIM/USIM) and non-mobile (e.g. PKI) technologies as well as biometrics.

1 Introduction

1.1 Worldbank

The Worldbank supports countries in many areas, including through the use of focussed ICT deployment. For this purpose, Worldbank identified three ICT Strategy Pillars: transform, innovate and connect. 'Transform' aims at making development more open and accountable, and at improving service delivery. 'Innovate' addresses the developing of competitive IT-based service industries and the fostering of innovation. 'Connect' focuses on afordable access to broadband.

1.2 The Toolkit

In 2012, the World Bank launched a study to create a toolkit on secure eID systems. The toolkit aims at giving practical know-how to African governments on building national eID systems that can help deliver social services on mobile platforms. PricewaterhouseCoopers was invited to conduct this study. The Toolkit is expected to be publicly announced in the second half of 2013, most likely in a potential pilot country.

The project includes technology and regulatory assessments (at global, regional and national level), the creation of selection criteria for African launch country, deep dive case studies, interviews and on-line collaboration [LinkedIn].

The project is structured in three phases: conducting interviews, performing an eID scan, and Toolkit elaboration. This should be followed by one or more pilot implementations, and subsequent deployments.

2 Interviews

The study started with interviews in East, West and South Africa, as well as Europe. Managing Directors from various national identification authorities as well as from ICT promoting entities and regulatory bodies were interviewed.

Even though the national ID infrastructures in the studied African counties are in different development stages, all the interviewed government officials agree that the usage of mobile eIDs would be beneficial for their countries. They see it as an opportunity to provide a variety of government services, such as voting, taxation, or social services. As the main advantage of such solution, they emphasise a relatively high mobile phone penetration, even in rural areas, which would enable high availability of the offered services. As one of the key requirements of a future eID solution, they highlight the fraud detection and prevention, which would provide trustworthiness of the government services. On the other hand, the government officials share concerns about the infrastructure problems, such as lack of electricity in some areas, low level of technical education of their citizens, low security and privacy awareness, the lack of regulatory frameworks and a low level of collaboration between the mobile network operators.

On the other hand, the interviewed eID experts, coming both from academic and industry backgrounds, express a general agreement that the existing eID technology is able to mitigate many of the identified risks, especially the ones related to security and privacy. However, the consensus is that the technology must be properly managed, supported and regulated. For instance, binding a Subscriber Identity Module (SIM) card to an individual or the existence of a civil registration system are the prerequisites for a valid mobile eID scheme. In case a single eID registry is lacking, information might be provided from other registers such as Election Committee Registers and Registers of Births and Deaths.

The eID experts all share the view that it is necessary to tailor the eID solution in order to meet the country specific needs. Therefore, it is important to come up with a generic solution which offers a wide set of options and to use it as a starting point for customization of the country-specific solutions. In order to do so, it is important to refer to the successful eID projects such as the one in Sri Lanka, but also to the global examples of successful eID roll outs. By learning from their experience and the variety of offered solutions, it would be possible to define a generic solution that could capture the needs of all the countries in the scope of the World Bank Study.

The experience for the Mobile eID scheme in Africa can be gathered from multiple approaches and technologies used for the national eID projects worldwide. The prominent examples are the "driving licence" based identification used in UK and USA, and the various EU approaches offering examples of smart card, soft certificate, mobile or even username/password based identification schemes. Another approach that is particularly interested is the Indian UIDA approach, due its focus to enrol people from rural and underprivileged communities, and its large scale use of biometrics.

1 eID scan

Parallel to the interviews we conducted a stock-taking study on the current eID landscape. The goal was to take stock of the current and the emerging uses of eID and good practices around the world, and use these experiences as guidance to identify the major hurdles when adopting eID. Particular focus was on how these experiences where changing the traditional approach to public service delivery and accountability. The scan addressed:

1. eID overview. This part summarizes the main uses of eID in US, EU, India, and Japan and describes their different approaches to eID according to their particular situational factors (i.e. cultural background, technical means, resistance, ..). Subsequently the main applications of eID today are summarized (i.e. e-identity, e-banking, e-passports, e-ticketing), and the business models used (i.e. government driven, commercial, partnerships...).

2. Major technological trends in mobile eID. The "mobile electronic identity" was identified as an approach which holds a great potential to the African situation thanks to its capacity to be "portable" and self-contained. We reviewed the different types of mobile eID credentials (smart cards, USIMs, Secure Elements) and the technical solutions allowing implementation of them (mobile phone based, Server based, Software based or Token based)

3. Case studies. To gain an understanding of the experiences of successful eID implementations, a number of case studies on the introduction of eID at the national level have been conducted. This includes five high-level cases on Austria, Belgium, Turkey, Finland and The Netherlands as well as three deep-dive case studies on Estonia, India and Nigeria. These were selected because they are either "success stories" in the field of eID (e.g. Austria, Belgium and Estonia) or because of the similar economic and socio-cultural factors to African countries (i.e. India or Nigeria).

   The deep-dive studies provide a combination of historical background, strategic choices, actors constellations and business and implementation models that allows for the explanation of some, but by no means all, of the complexities related to the adoption of a national eID. The studies provide as well an analysis on the "practical implementation" of the respective eID systems in the countries under studies, including details on the legal and technical frameworks put in place.

The main lessons that we can draw of this analysis are:

- A successful combination of private-public partnership can lead to the provisioning of services that make use of trust services both in private and public sector. A broad service catalogue contributes to the adoption by a broader public.
- The adoption by broad sectors of the population is a fundamental step forward towards the success of a national eID program, and public awareness campaigns play a key role in overcoming any initial resistance and enhancing the adoption of eID services by the population.

The size of the population is a significant factor. In Estonia, the implementation of eID systems has been relatively fast (partly due to the adoption of consolidated commercial eID solutions). In the Indian case, given the size of the population, the technical resources mobilized are huge, but still covering the whole country remains a daunting task.

3 Technology aspects

1.1 Core assumptions

The eID solution should be based on an Identity Repository that is operating according to government regulation. This repository should contain all identities of citizens, and optionally of registered foreigners. In case a Mobile eID (MeID) approach is taken, this solution will base itself upon/link to a subset of the full identity repository. We assume that the selection of the credential medium (e.g. smart card, SIM in a mobile phone, etc) will be a consequence of the envisaged eID functionality. In case an MeID solution is selected, it should be possible to establish multiple mobile identity repositories (M-IDREP), to cater for multiple Mobile Network Operators (MNOs). Such M-IDREPs should not interfere with the normal course of business of the MNOs and their current Home and Visitor Location Registers (HLR/VLR).

1.2 Assumptions with regard to technology

It is commonly accepted that achieving absolute security is impossible. The state-of-the-art is typically illustrated by a leap-frog situation, where new security solutions are constantly challenged and attacked. Some solutions stand for a long time, others not.

People can be coerced or bribed, and as such may insert an element of insecurity in a system. Even if one would design, manufacture and deploy a perfectly secure smart card or SIM for identity purpose, the people involved in the production chain still remain vulnerable to various types of non-technical attack. Furthermore, people might evade the use of technology if they do not see the benefit or if they seek to avoid side-effects e.g., when technology threatens their privacy.

Electronic ID cards and passports are traditionally based on PKI and document security. However, as technology continues to evolve, governments may prefer to make use of emerging technologies including those commonly referred to as Privacy Enhancement Technologies (PETs). We assume that credentials (including private keys) should be stored on a mobile device (alternatively on a traditional Personal Computer, a traditional Smart Card or a Host Security Module (HSM)). The credential store should be adequately protected in function of its use.

Finally, the information on the card/saved in the chip is an authenticated copy. The master copy of the information is stored in the identity repository. This master database can be a real or a virtual database, i.e., distributed over various organisations.

1.3 Technology foundation

The technology foundation includes:

- eID applications for use by personnel to capture citizen information;
- Back-office IT infrastructure and eID database;
- Communications infrastructure for linkage of eID central office with field offices;
- ID mediums such as smartcards (and possibly mobile phones); and

- Authentication and POS devices (including biometric devices, smartcard readers, etc.).

A solution based on this foundation leads to the following high-level framework:

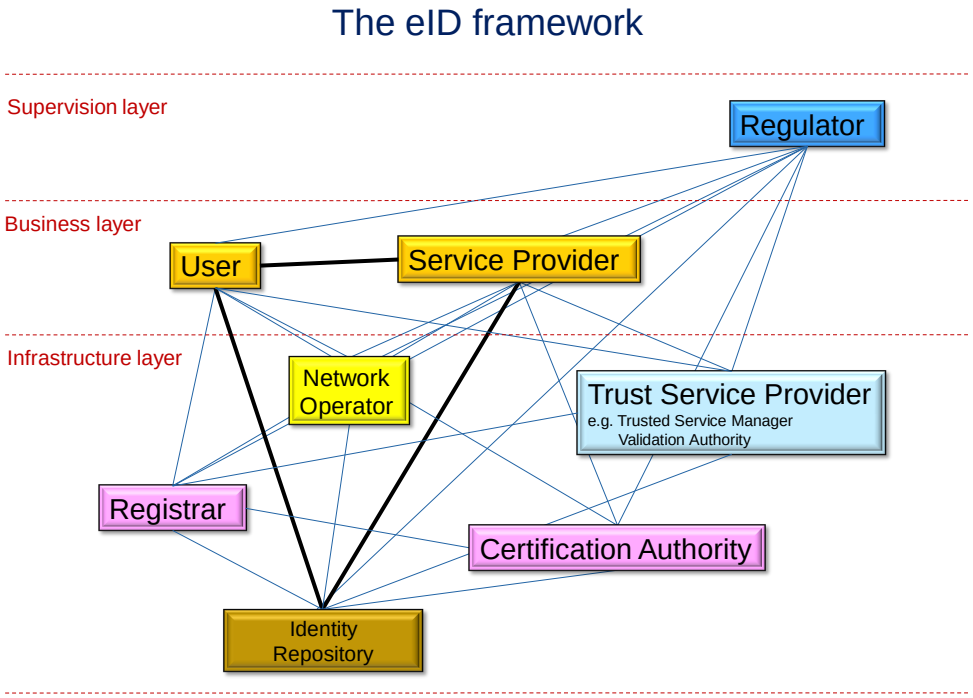

Fig. 1: The eID framework proposed by the Toolkit

In the case of a Mobile eID scheme, the above actors are complemented by the mobile identity repository, and one or more MNOs, enabling the communication, and optionally also fulfilling other functions (potentially acting as Registrar, as Certification Authority, as Trust Service Manager[1] or Trust Services Provider).

1.4 Core technology activities

We now briefly discuss the core technology activities that need to be performed to implement the landscape illustrated above. Complementary activities are addressed in the Toolkit but not discussed here.

1.4.1 eID scheme and responsibliities

Based on the objectives established by the stakeholders, the functionality of the eID scheme and its issuer need to be defined. Key elements include design and definition of:

- The roles, responsibilities and liabilities of all participants;
- The issuer function;
- The types of credentials that will be supported.

[1] We use the notion of TSM as defined by Global Platform

Roles, responsibilities and liabilities of all participants need to be defined. Functional services offered under the eID Scheme, and types of applications envisaged to be supported by the scheme should consider: business goals, issuance and full lifecycle of the eID and its supporting credentials, including approval and support for the credentials on the network and on the phone or other deployment platform. Furthermore the operation of the infrastructure (identity repository, CA, Trust Services Providers, TSM) and development and support of applications should be defined. Key elements to define include:

- Desired legal effect, and relationship with legal context, laws and regulations;
- List of participants, and the roles and R&L of these participants;
- Conformity assessment requirements on trusted hardware/software;
- Technical standards;
- Trust model and validation rules.

As the issuer is fundamental to the eID scheme, this function needs careful design. The issuer may or may not group elements of the various functions such as Registrar, Mobile Identity Repository, Identity Repository and Trust Services Provider. The issuer function can be fulfilled according to many alternatives, including by a dedicated legal entity, a government institution, and a Mobile Network Operator. It may be organised in a centralised or decentralised model. Each model has its strengths, weaknesses, and associated costs. A centralised model allows easier control over safeguarding the breeder documents, but may require citizens to travel a long distance, or may require careful planning to avoid long queues. A decentralised model is closer to the citizen, but requires decentralised personalisation equipment, which comes at a cost. Obviously, combinations are possible. The following briefly describes a combined issuing approach:

- A citizen is sponsored by someone from a local issuing office (or someone who has a relationship to it). The citizen then receives an email saying they've been invited;
- The email contains a link for the individual to schedule an appointment at a registration office;
- During the scheduled appointment at the registration office, the citizen's enrolment documents are verified and his biometric information captured; Information from complementary registers such as an Election Committee Register, a Register of Births and Deaths, a Social Security register, or a register from a Utility company or an MNO may provide additional background;
- The office adjudicates an individual by performing a criminal history check. Subsequently the office issues a request to a central function to personalise the credential;

- The credential is personalised and shipped to the location specified by the citizen's sponsor. The citizen is notified and asked to make an appointment to activate and pick up the credential;

- The office finishes the electronic personalization of the credential and loads the certificate and biometrics to the chip.

Care should be taken to balance the issuer's responsibilities with its liabilities. For example, when the issuer has no or very limited control over the registration process, the types of credentials, or the CA and Trust Model, his liabilities need to be clearly described and documented.

Obviously, there are many alternatives possible with regard to the credential. Traditional Smart Cards are a popular type of eID credential. They have the disadvantage of requiring a reader, which often means a PC or Kiosque is needed, as well as the installation of a device driver and sometimes some middleware (which adapts the card's software architecture to the business application). SIM cards are another popular credential. Traditionally, the mobile infrastructure belonged to a MNO, was dedicated to its traffic, and could be considered a closed system. In GSM/3G, the authentication mechanisms such as Authentication and Key Agreement (AKA) assumed an implicit trust relation between the Authentication Centre (AuC) and the VLR/SGSN, and a trust relation between VLR/SGSN and the subscriber based on the shared key K. However, to achieve identity authentication and non-repudiation in an Internet ecosystem we need to introduce some form of asymmetrical credential. For this there are many different approaches possible. An asymmetrical credential (typically including a private key) could be stored in a credential platform under local control of the Citizen:

- In the UICC, which is typically owned by a MNO. This would imply that the MeID on-card application would be provided by the government and the UICC should be multi-application UICC, and the MNO would accept responsibility for the lifecycle of the MeID application onboard its UICC;

- In an embedded Secure Element, which should preferably be multi-application, since it cannot be relied upon that a dedicated handset will be manufactured and maintained to support the MeID application for a particular country only; the responsibility for the lifecycle of the MeID application should then likely be agreed with the handset manufacturer, or a TSM-style solution should be implemented;

- On a secure µSD card, which could either be single (MeID–only) or multi-application. In this case, the responsibility for the MeID application's lifecycle should be defined;

The credential could equally be stored under control of the Citizen, but also in a centralised authentication or signature engine; Furthermore, for Internet application protocols, through the use of 3GPP GAA/GBA and its interworking architecture with the Liberty Alliance, OpenID Connect, or similar protocols, asymmetrical protocols could be leveraged.

As there are many alternatives possible, we refer to these in general using the name 'credential platform'. The eID Scheme may also select a 'virtual' credential, i.e., it can define high-level eID specifications, and certify various implementations on different platforms. The eID Scheme may also propose different levels of security, such as STORK's four different QAA levels. This would on one hand allow citizens to select the credential platform

they prefer, while on the other hand allow Service Providers to specify minimal security levels for their applications.

1.4.2 eID business applications and credentials

Applications are capable of consuming eID services need to be defined. These can be both "stand alone" (using your credential without network connectivity) as well as integrated in other electronic transactions. Typical applications may include e.g.:

- Confirmation of identity (authentication);
- Recognition of life-events (birth, marriage, adoption, divorce, death);
- Identity as enabler: access to services and benefits, with NFC also access to physical locations;
- Confirmation of attributes: „I'm over 18", „I have the right to access this information, including e.g. a drop box", „I have paid for this service", „I can participate in this group".

From an eID perspective, there might be specific requirements on the citizen that are function of the selected technology, e.g. a Smart Card will require a reader (which needs to be connected to a host platform). The reader can be contact or contactless, in function of the selected card. The reader will establish the communication between the on-card application and a host application, e.g. residing on a Personal Computer, or on a Server. From a Mobile eID perspective, there are no specific requirements on the citizen, except the assumption that he/she is registered in the identity repository, has a mobile phone from an MNO participating in the MeID scheme, and a matching credential platform (typically the right type of SIM). It should be decided whether requirements for accessibility (e.g. blind people) should be taken into account. There are at least two main alternatives.

Alternative 1 Asymmetric credential on the phone

The credential platform could be implemented in the UICC, which may store the MeID credential. It is common to distinguish between the SIM, the UICC, the USIM and the ISIM:

- In 2G GSM, the hardware (ICC) and software (Subscriber Identity Module) are tightly integrated and the abbreviation SIM was typically used to refer to both aspects together;
- In 3G, the hardware is referred to UICC, while the UMTS SIM is referred to as the USIM (Universal SIM) and an IMS (IP Multimedia System)-capable SIM is called an ISIM;

As many UICCs are now multi-application, it is possible to load applications onto the card after distribution, typically via OTA (Over The Air).

Alternatively, the credential platform may be implemented in a Secure Element, in a secure µSD card, or equivalent solution. Java Card and MULTOS became popular implementation

bases for such a Secure Element. It is relevant to consider the Global Platform suggested approach[2,] where a Trust Service Manager (TSM) governs the installation of applications on-card. There can be multiple security domains for multiple application issuers, all coexisting on the same physical card.

Alternative 2 Asymmetric credential on a central server

The asymmetric credential may alternatively be stored in a central HSM, and the mobile phone then authenticates against the central server. In such a set-up, the user authenticates himself against the phone (e.g. with a PIN), which enables the usage of a symmetric secret key stored on the phone. Please note that this is typically a dedicated key, and not the key K from the phone, since this one is reserved for MNO phone-to-network authentication. Using the symmetric secret key on the phone, the user authenticates himself against the central server. The central server delivers an authentication ticket to the application that the end users intend to use.

Obviously, for a particular country it may be relevant to offer both alternatives. This would allow the citizen freedom of choice, which leads to higher adoption rates.

Local applications

The stand-alone application on the phone should allow identification and authentication of a citizen. This should support:

- First line inspection, an examination done without tools or aids that involves easily identifiable visual (or other) features for rapid inspection at the point of usage;
- Second line inspection, an examination that requires the use of a tool or instrument (e.g., a reader, a scanner, an application) to discern a genuine from a fake credential; in case biometrics would be stored within the credential, these could be read out and compared to a life capture;
- Third line of inspection, an examination in a specialised laboratory. In-depth logical and physical inspection of the identity safeguards by experts.

On-line applications on the phone follow the client/server model, and consider the application-level protocol stack (SMS, TCP/IP, or a combination).

1.4.3 Service Provider MeID applications

A service provider can be defined as a private or public entity (or a combination) that offers a certain service to a citizen. This service could come in the form of a browse-able website or the server part of a client/server application (either through SSL or through signed or encrypted SMS). This can be freely chosen by the service provider.

The service provider can make its service available through an **SSL enabled website or server application.** When the service provider makes an SSL-enabled web site or server application available to a citizen, PKI/SSL good practices should be followed. It is up to the

[2] The integration of the ETSI framework and the Application management framework of GlobalPlatform is standardized in the GP UICC configuration

service provider to ensure that the functionality offered by the website or application is viewable on the citizen's device. If a service provider opts to use an application rather than a website, it is up to the service provider to ensure that the application is made available to the citizen. Service providers could also publish a service that can be accessed through the **signed or encrypted SMS**, which would eliminate the need for IP-based network connectivity for both citizens and service providers. The citizen would sign or encrypt an SMS, using one of the private keys contained on his SIM card, and send the SMS to the service provider. Again, PKI good practices should be followed.

1.4.4 The eID infrastructure

As the design of the eID infrastructure depends on the vision and scheme, we will discuss only the key aspects of the most important components. The **identity repository** is preferab ly under control of the government. It contains all relevant information about a person required by legislation, such as name, gender, address, possible biometric information such as a photograph or fingerprints. Each person is identified by a unique identification code. This identification code (or a derived pseudonym) can be used to link with other databases (for example MNOs, health service providers, etc.). The need for anonymous or pseudonymous services should be considered here. The identity repository may include the **registrar** functionality. It may equally include the required **CA** functionality such as cryptographic root keys and citizen's certificates. In case the CA functionality is not included in the identity repository, it can be provided as a service.

The **Mobile Identity Repository** and its relationship with the identity repository should ensure that all information contained in the M-IDREP should be accurate, integer and synchronised with the identity repository. It should respect privacy regulations, and all information contained within it should be adequately protected. The M-IDREP would make use of the citizen identity repository, but would not be part of it. It is better to separate the two, as they both serve a different purpose: the citizen identity repository would eventually contain information about all citizens, and can be used by a variety of applications. The mobile identity repository would be used solely for registering and issuing the subset of mobile ID's. For the Mobile Network Operator, key aspects to be addressed include:

- Type of SIM/UICC in use;
- The MNO's willingness to move to other cards if required;
- The choice whether the MNO will act as the Issuer or not;
- The relationship between the MNO and the TSM;
- Importance of key renewal.

The **Certification Authority** is used to securely create, manage, distribute, use, store and revoke digital certificates. Among its many components, it typically includes the core Certification Authorities components such as the root and operational keys and signers, the Registration Authorities (RA's) and web services where the CRL or OCSP can be consulted. A CA can be considered as the entity that actually creates, signs and issues certificates, while the RA only performs registration-related tasks on behalf of the CA. Generally, it enters into

an agreement with the CA to collect and verify each subscriber's identity and information that is to be entered into the certificate. In the MeID scheme, the CA can operate its own RAs, or can make use of the registrar's function of the identity repository. The CA would be used to offer certificates both to citizens and certain applications. Of course, it would offer standard services such as OCSP checking and CRL publishing. Under no circumstances should the CA have access to a citizen's **private key**. A citizen's private keys should remain in the sole possession of the citizen, securely stored on his or her mobile device.

With regard to Trust Service Providers, what is required depends on the vision, scheme and selected Trust Model.

4 Sample application of the Toolkit's framework

Worldbank, together with its partners and sponsors, envisages the launching of the toolkit in a specific country. To improve the probability of a successful outcome of such launch, reflections were made on those issues that need to be addressed prior to a launch. These include the existence of an appropriate regulatory framework, including supporting laws and civil repository system, as well as public private partnership (PPP) model. Other issues are the existence of a national identity database, mobile network operator collaboration and ensuring that the objectives of both government and private parties are met. Furthermore in case a mobile phone-based solution would be selected, extensive mobile penetration, portability of the mobile phone numbers between the mobile network operators, and the security of the networks as well as of the SIM/USIM need to be considered. The list of potential candidate counties include but is not limited to: Nigeria, Ghana, Rwanda, Gabon, Senegal, Togo, Ethiopia, Tanzania and Burkina Faso.

When evaluating the situation in a potential candidate country, following points can be expected to require particular attention. At the supervision layer, the existence of multiple registers is often reflected in silo legislation. Furthermore, eSecurity (eg cryptographic functionality for authentication, signature, validation, etc) is often not sufficiently regulated to support legal effect of electronic transactions. Electronic credentials are not commonly deployed, and eGovernment applications may be limited. There might be no local CA or TSPs, and there might be no single reliable source of identity and authentication. On the other hand, there might be many partial such sources, each focussing on specific parts of the population (birth, election, healthcare, death, passport, ...).

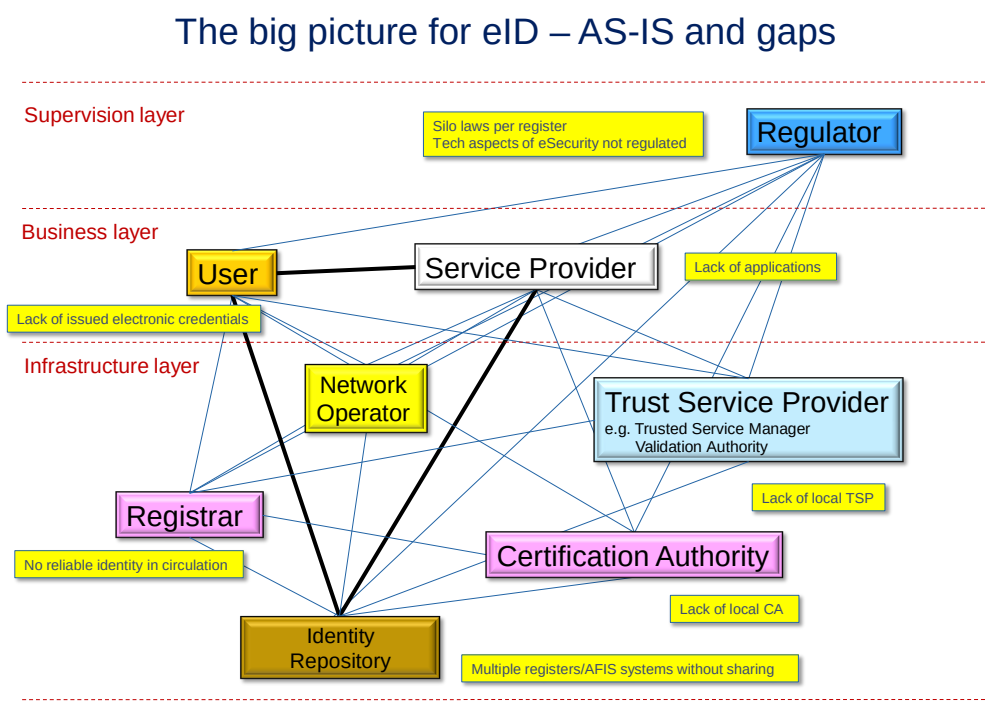

Fig. 2: The eID framework with sample gaps

The framework can then also be used to identify the key activities that need to be undertaken. At the supervision layer, the Supervisor's mandate may have to be extended to cover all relevant aspects, and eSecurity standards are to be defined and enforced. At the business layer, the [M]eID credential is to be deployed, and eGovernment services should be available in those areas offering most value. At the infrastructure layer, CA's and TSPs need to be established, and the Registrar function of the CA should make use of the possible cross-reference information that can be offered from the various registers such as Birth and Death, and potentially any other available registers. Finally, a recognised authentic identity register should be established as the foundation.

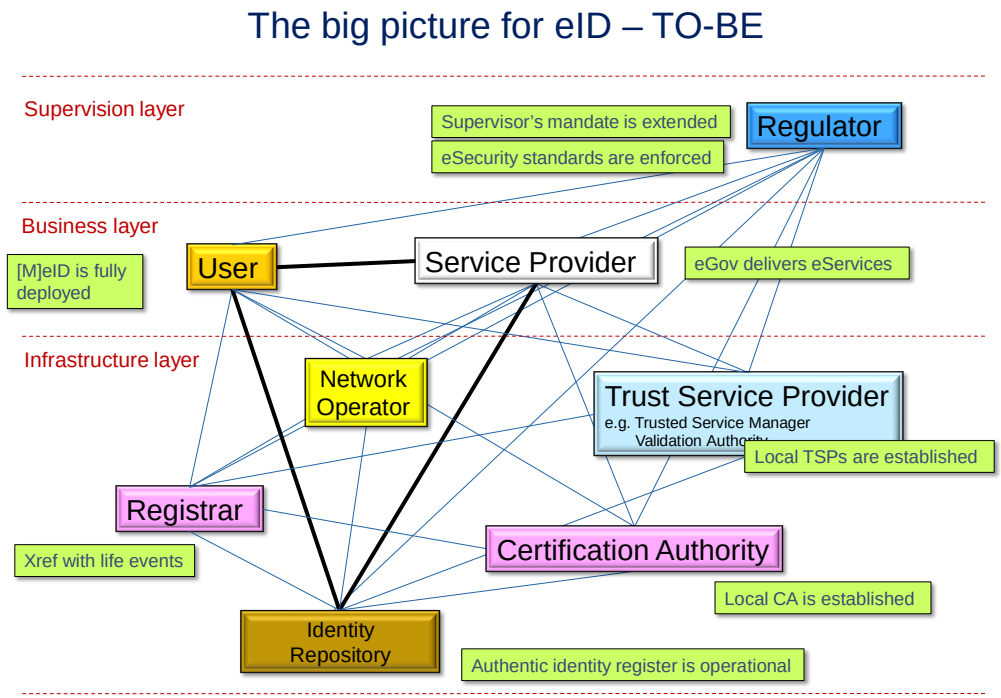

Fig. 3: The eID framework with sample actions

5 Conclusion

With regard to the key technology features of a [M]eID solution, the Toolkit proposes a framework model to allow the distribution of roles and responsibilities of the various stakeholders and participants across different layers and components.

The eID Scheme may select a 'virtual' credential, i.e., it can define high-level eID specifications, and certify various implementations on different platforms. The eID Scheme may also propose different levels of security, each of which can be implemented on different platforms. This would on one hand allow citizens to select the credential platform they prefer, while on the other hand allow Service Providers to specify minimal security levels for their applications. In order to offset some of the challenges of the Registrar function, cross-referencing with well-established registers is recommended.

It is recommended that a country applying the toolkit should strive to organise an implementation project in at least three parallel tracks that should have common objectives. Implementing technology should go hand in hand with implementing the business model(s) and applications, as well as the required regulation.

References

[LinkedIn] LinkedIn group: http://www.linkedin.com/groups?gid=4627623