IST-Africa
IST-Africa 2015 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2015
ISBN: 978-1-905824-50-2

E-identity: Basic Building Block of e-Government

Jiří PRŮŠA
CZ.NIC Association, Milešovská 1136/5, Praha 3, 130 00, Czech Republic
Tel: +420 222 745 111, Fax: +420 222 745 112, Email: jiri.prusa@nic.cz

Abstract: Creating a system of electronic identification and authentication represents one of key prerequisites of successful and efficient e-Government that will offer to citizens and businesses comprehensive processing of their requests without the need to physically visit the office. The United Nation, within their regular evaluation of e-Government development, reviews the availability of individual electronic services as well as their sophistication. If public administration wants more than just to provide information and aims to offer its customers higher quality services in the form of transactions or even interconnected services, it will sooner or later try to solve the e-identification issue.
Experience of some EU member states and experts' recommendations show that the only e-identification tools with a chance to succeed are those that are simple, user-friendly and allow logging into e-services of both public and private sector. Among those tools, without any doubt, is mobile eID whose potential is to be unlocked especially in Africa, which has become a pioneer in mobile payments and other intelligent services using the widely spread mobile phones. Besides mobile eID a successful identification and authentication tool may also be represented by cards issued in cooperation with banks (payment card issuers), as is the case not only in Europe (e.g. Sweden) but also in Africa, e.g. in Nigeria. Interconnecting of public and private services then brings also the question of attributes' (credentials') trustworthiness, where the level of trust in a given instrument is derived from the sensitivity of the service and the amount (level) of personal data that are required. For some services, e.g. enabling access to budget information or elected representatives' voting, a basic authentication is enough, to set up a business or to change a residence, more reliable authentication will be required.
Together with the increasing mobility there is the possibility to use eID issued in another state and thus enabling easy, simple and fast handling of official matters (including e.g. tax payments) also to citizens of other states.
This paper aims to evaluate the European experience with the tools of electronic identification and authentication, building a cross-border system of electronic identification within the STORK and STORK 2.0 projects, including setting a scale of trustworthiness and respecting national solutions and providing inspiration to African states with building electronic identification as one of the basic building blocks of e-Government.

Keywords: e-Government; interoperability; electronic identity; eID; cross-border; STORK; eIDAS;

1. Introduction

The identification of citizens via state-issued documents is nowadays one of the core activities of most of the world's public administrations. The ID document in itself, which enables the citizens to identify themselves while dealing with public offices as well as other institutions-e.g. banks, car rental offices etc., nevertheless represents only one part of the system. The other part, the so-called back-end and 'invisible' to the citizens, is represented by a population register in which a state records basic information about its citizens,

especially given name, surname, permanent residence address and the number of the ID document issued.

As the information society develops the need for identification shifts more and more into the Internet realm. The basic need to verify the identity of the users is the same in the electronic world as in the physical one–a trustworthy identification that the recipient of the services (electronic services, in this case) is truly who s/he claims to be. Such verification is important for accessing the public administration services (e.g. public administration portals, filing tax returns, supporting/signing a petition, accessing medical documentation …) as well as the private sector services (e.g. Internet banking access, e-shop purchase or ordering carpooling). More detailed information about the need for electronic identification and the added value of trusted electronic identification are provided in chapter 5. – Business Benefits.

Hand in hand with the increasing mobility (including the cross-border one) comes the issue of using eID issued by a different state and thus enabling simple and fast processing of (not only) official matters to citizens of other countries. Considering the often different technological solutions (see Chapter 3.1. Basic technological solutions for electronic identification) there arises the need to solve interoperability not only technical but also legal, especially in relation to the accountability of the data provided.

Nowadays Europe represents the unequivocal leader in the area of mutual recognition of eID tools issued in another state, as it has started with connecting individual national tools and creating a functional framework for interoperability of electronic identification and authentication, based on the adopted strategic documents–especially the Digital Agenda for Europe [1] and the European e-Government Action Plan 2011-2015 [2].

To verify the feasibility of cross-border electronic identification and to demonstrate the advantages of eID interoperability, since June 2008 the European Commission supports the implementation of the STORK project (Secure idenTity acrOss bordeRs linKed) [3]. Since April 2012 the follow-up STORK 2.0 project [4] aims at the development of infrastructure for mutual recognition of eID as well as at involving non-state stakeholders such as universities or banks, both as recipients (users) of trusted electronic identities and as providers of attributes.

The legal basis for the mutual recognition of electronic identification and authentication tools among individual European countries was laid down in July 2014, with the European Parliament and the Council adopting Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the so-called eIDAS). Besides the area of electronic signature and qualified certificates this Act also rules on electronic identification and authentication and on mutual recognition of individual e-identification tools, that will become commonplace in Europe in 2018. The eIDAS Regulation therefore represents another step towards creating the so-called Single Digital Market and thus points out a problem that is relevant not only in Europe but also in Africa.

While the common (physical) identification documents such as ID cards or passports are recognised as a basic identification tool without any problems e.g. at a border control, accommodation in a hotel, car rental, or a roadside check, the holders of electronic identification documents do not benefit these advantages and the validity of electronic identification is usually restricted within a certain state or to the institution that has issued such a document.

2. Objectives

The goals of this paper are especially:

1. To assess the current possibilities of electronic identification, and to evaluate success cases from Europe and Africa with recommendations on the future direction of the eID development;
2. To show actual business cases for electronic identification in both private sector and public administration;
3. To stress, in light of the increasing mobility, the importance of mutual recognizing of eID tools issued in other states and to offer some business cases for trustworthy electronic identification and STORK 2.0 in African countries;
4. To assess the European experience with creating cross-border electronic identification system within the STORK and STORK 2.0 projects, including setting a scale of trustworthiness and respecting national solutions.

3. Technology Description

The technical aspects of electronic identification can be divided into national solutions including the state-issued documents (esp. electronic ID cards) and the tools of the private sector (esp. tools for logging into electronic banking), and technological solution of individual national systems‘ interoperability for the purpose of mutual recognition.

3.1 Basic Technological Solutions for Electronic Identification

At this time there is no standardised electronic identification solution that would be used universally, by all states. The use of a specific electronic tool is influenced by the circumstances in which the individual national solutions emerged, e.g. with regard to the historical and constitutional conventions (e.g. in Great Britain).

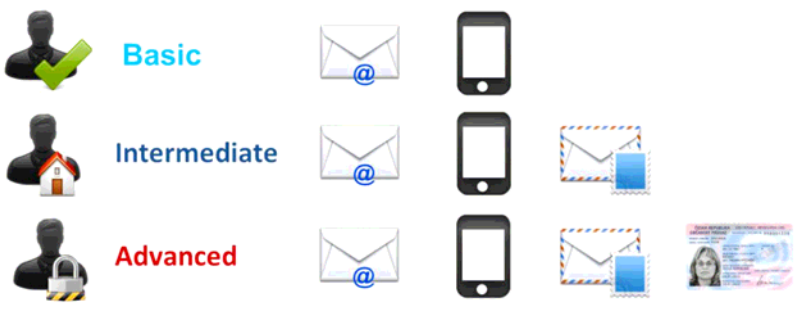
Based on a comparative analysis of individual member states the electronic identification tools can be divided into the following groups, and the detailed information including assessment of experience and costs in selected EU countries can be found in the „Smartcard eID Comparison“ document [5], which was developed under the STORK project. Within STORK 2.0 there was also produced an up-to-date list of eID solutions [6], (based on both qualified certificates and mobile platforms).

- **Solutions based on qualified certificates** – as part of the solution the user has a chip card that can be visually similar to common identification document (e.g. ID card), the only difference being the location of the chip on which is placed the certificate using a public key infrastructure (PKI). For security reasons there are usually two certificates on the card – one for signing and the other one for authentication. With regard to the trust (that is often also anchored in the legislation) the issuer of the certificate is an important person. It is usually one of the qualified certification authorities, whose function can be in some cases also carried out by a state organisation.
  However, in some European states (e.g. Sweden) as well as in Africa (esp. Nigeria) are also used certificates issued by banks or companies issuing payment cards. In Luxembourg, banks and governments share infrastructure costs and eIDs have multi-applicability – access to electronic service operated by public (municipalities) and private sector (banks) as well. However, as the public side sets up standards, the private sector has to obtain certifications. Government eIDs can be a threat to the private sector as the private sector develops devices, sells them and also makes money on their use by the users.[13]
  The largest rollout of a biometric-based verification card with an electronic payment solution in the country and the broadest financial inclusion program in Africa was launched in 2014 in Nigeria. In the pilot phase, the Nigerian Identity Management Commission (NIMC) will issue MasterCard-branded identity cards with electronic payments functionality to 13 million Nigerians [7]. Such a solution is advantageous especially for countries whose citizens widely use payment cards. In case of Nigeria, according to its central bank, about 30% of the country's 167 million inhabitants have

access to bank accounts. The indisputable advantage of this solution is the possibility to use a single tool for logging into one's bank (an example may be Sweden and the Nordea bank) as well as for e-Government services and possibly other services also, such as e-shops. A disadvantage is the requirement to own (and install) a chip card reader and to enter (register) the certificate into a web browser or other programme, e.g. email client or document management system (DMS), which places increased demands on computer literacy of the individual users. To use the eID function online, a citizen needs a certified card reader. Prices range from EUR 25 for basic readers without a PIN entry keypad to EUR 160 for a multipurpose reader with display and keypad that supports other smart card applications as well. Uncertified readers cost few EUR. In case of collaboration with banks it is necessary to pay increased attention to personal data protection, as just in the case of Nigeria the watchdog organisation Privacy International pointed out [8] that partnership with MasterCard puts personal data at risk and could exclude millions of people.
Other cards can be used as well, be it student cards or health cards.

- **Solutions using mobile phones –** these solutions using mobile phones' infrastructure may be based on infrastructure integrated into SIM card (e.g. Iceland's Skilriki service) or they may use a one-time password sent to the phone, similarly to electronic banking, with a two-tier authentication: first via a username and password and then by entering the password sent to the mobile phone. An integral part of this type of authentication is being sure that the password is sent to an owner's verified number. The Estonian and Austrian experiences show a high popularity of this solution, which is much more user-friendly than chip cards for the citizens. With regard to the success of mobile solutions in Africa [9] it can be reasonably assumed that mobile eID issued e.g. in cooperation with banks or other entities (see below) would find a positive response in African countries and help to a significant and qualitative improvement in e-Government.
- **Single-sign-on systems built on a software basis –** a condition for use of these systems is a user registration on the operator's web page, with the possibility to use the user name and password to log into other operators' electronic services, both public and private. For security reasons these systems then use single-factor authentication using a user name and password, as well as multi-factor authentication where the user name and password is supplemented with other authentication, either via a one-time SMS (similarly to mobile eID, see above) or via a one-time password (OTP). If the operator demands it, it is possible to e.g. via a SAML protocol exert also a login via a certificate.
In order to build trust these systems allow further verification of users. An example of such an authentication can be the Czech service mojeID operated by the CZ.NIC Association, an operator of the national .cz domain. The mojeID service provides the following levels of identity verification which vary in the degree of quality of the registration process.

Graphic 1: mojeID Levels of Trust



For the Basic level it is necessary to enter a code received via e-mail and text message to a mobile phone, for the Intermediate level the activation code is sent by post to a physical address and for the Advanced level the data are verified based on a valid physical identity card or passport. The most important personal attributes (First name, Family name, Date of Birth, and Permanent Address) are verified during the Advanced level validation process. This validation process is made mainly by notaries and some self-government Register Offices. The verification can also be done based on an electronic application signed by advanced electronic signature.

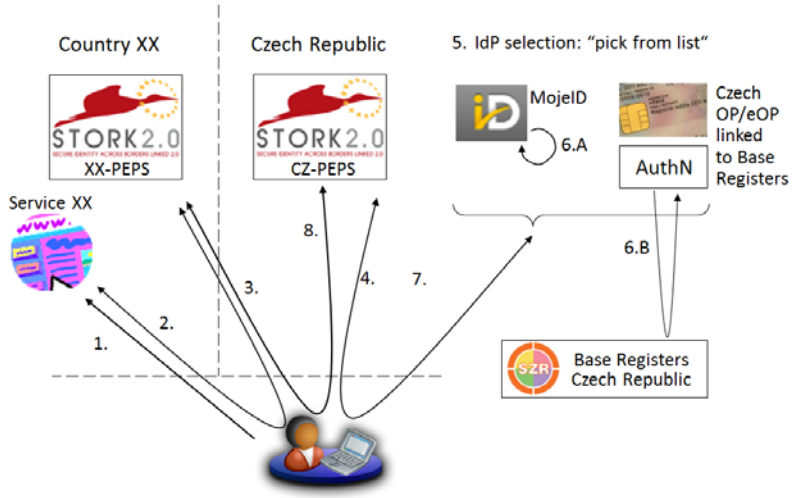
Besides the Czech Republic an example of a single-sign-on solution may be e.g. the Dutch DigID service [10].

3.2 Technical Solution of Cross-Border eID Recognition

There are two approaches to ensure cross-border interoperability. The first one envisages the use of common standards and solutions, which will then be possible to easily connect and thus create federated services. Given that individual states, however, opt for various systems for electronic identification (see above) not only in terms of technical solutions (e.g. type of cards) but also of the entire philosophy including links to national registries and the range of the attributes provided, in Europe the STORK project chose a solution respecting the individual national systems.

This solution is based on a system of interconnected and communicating proxy servers (so-called PEPS), to which are then connected national eID tools. At the same time, every member state can customize this solution according to their needs. This technical solution is based on open standards and the implementation on open source code. Both things will allow easy integration of the common modules for interoperability of eID with any type of technology that can be found in the market, favouring therefore the scalability of the solution and the extension of it to any European member state. The architectures and models for interoperability of eIDs that will be chosen will be based on those developed in the STORK project, and any enhancement or amendment of them will continue preserving the principle of scalability, defining solutions that can be easily and efficiently extended to other EU countries [11]. The principle of operation linking national identities, using the example of the Czech Republic, is illustrated in the following diagram:

Graphic 2: STORK 2.0: Principle of Operation Linking National Identities



4. Ensuring Trust Within Electronic Authentication

To ensure the operation of mutual recognition of eIDs across individual states, the issue of trust, along with the technical solution, occupies a key role. While in case of national solutions the trust in the document is guaranteed by the issuing institution, in cross-border relations it is necessary to deal with different national conditions and with setting the conditions for issuing instruments at various stakeholders. The established system of trust should then take into account the requirements of individual services, as for the access to e.g. information services or e-Learning it is not necessary to put such an emphasis on credibility, as in the case of opening a bank account.

In order to establish mutual trust the STORK project created an evaluation framework, the so-called QAA (Quality Authentication Assurance). This model permitted quality levels to be assigned to various eID solutions, based on some of their main characteristics. The original STORK QAA framework [12] includes four levels of authentication assurance and allows rapid comparison of the assurances behind each eID, allowing service providers to select the most appropriate assurance level for their application.

The four levels defined in the QAA are based on various criteria that assess the organizational and technical characteristics of eIDs.

- Organizational aspects that must be taken into account are the quality of the identification procedure, the process of issuing identity tokens, and the quality of the certification authority.
- Technical aspects are related to the overall authentication procedure and include the type and robustness of the identity tokens provided and the quality of the mechanisms used for user authentication.

Each of these aspects is individually rated, and the weakest component determines the overall STORK QAA level for a certain eID.

5. Business Benefits

The advantages of electronic identification, and especially trusted e-Identification, are to be found everywhere where there is the possibility to misuse the anonymity of the Internet. The beneficiaries of this type of login are both end-users, who do not need to remember combinations of user names and passwords for individual services, but also the Internet service providers (ISPs), who receive verified information about who their users, respectively customers, are. At a recent discussion held by the European Commission, the representatives of businesses have agreed that an increasing business demand exists for trust, security and convenience in online transactions. The use of eIDs would provide for a more secure environment for cross-border business transactions[13].

5.1 Business Case of Electronic Identification

Based on the experience with operating the mojeID service in the Czech Republic and the experience in other countries, trusted electronic identity can be used mainly for the following types of entities:

- **E-shops**–online shopping represents one of the main activities of Internet users. According to Eurostat, 60% of Europeans shop online, including shopping in other countries. For end-users, a trustworthy eID offers especially the possibility of fast logging in to a shop without having to fill in the same data again and again. Single login significantly increases traders‘ conversion, as experience shows that as many as five per cent of customers leave an e-shop when asked to fill in registration data. These customers will not return to the e-shop in the future and its operators thus lose future profits. Another value added of trusted eID is the possibility to verify (confirm)

customers‘ identity when they do not pay by card, but by cash on delivery, whereby trusted eID minimizes the cases of goods being sent to non-existing address or non-existing person, in which case the trader incurs a loss in the form of delivery costs that represent, especially for larger and heavier goods (refrigerator, washing machine, furniture, tires), a rather high amount.

- **Academic services** – nowadays, the Internet represents an indispensable helper for students not only in Europe or in Asia, but also in Africa. Signing up for modules (seminars), learning the results of exams or logging in to e-Learning, all of that is today done electronically and necessitates electronic authentication. Due to the natural mobility of young people these issues are then solved not only within a single state, but also when visiting another university. The advantages of electronic identification in practice are shown in the already-mentioned European project STORK 2.0, one of whose pilot projects is aimed at academic services. The general objective of the pilot is to build on the outcomes of STORK a set of academic services that can be used by citizens, government and companies. Specific objectives of the pilot can be summarized as follows: 1) Build cross-border academic services based on the exchange of identity attributes (e-learning and opinion surveys); 2) Facilitate the use of academic information by government and private organizations (job qualification / selection [14].
- **Servers offering carpooling**–ride-sharing represents a welcome way of cost-effective travelling, especially for younger people. Moreover, it is often used cross-border. Due to more people being in the car and lowering the carbon footprint the drivers benefit both financially but also gain the advantage of e.g. a special road lane. To verify the credibility of drivers many servers use user feedback similar to e-shops. The example of the Czech server Jízdomat.cz showed that especially for newly-registered drivers it may be difficult to get the references, as users prefer drivers who have already been evaluated. As shown in this case, the solution may be a trusted eID that can replace missing customer references that -logically- a beginner driver simply cannot have. It has been proven that verification via a trusted eID is welcomed by several user groups (e.g. women students travelling to universities from their parents‘ homes), who feel more secure and minimize both the possibility of driver’s unreliability and of being abused.
- **WiFi operators**–in the interest of their own protection, and sometimes to fulfil the legislative requirements of some member states, some WiFi operators verify their users. The verification can be done by several means – from sending a code to e-mail or mobile phone to requiring a physical registration with an ID card/passport. A trusted eID solution may solve such a problem – the operators get easy user verification and the users easy and fast logging in.

5.2 Value Added for Public Administration

The advantages of electronic identification can be used in practically all the e-Government services. The main reason for each government to introduce e-Government and trusted electronic identification and authentication should be the resulting savings. Today, eID solutions, combined with robust application support for digital signatures provide a compelling foundation for continuous process improvement and cost savings. Similarly to a bank or an insurance company, in the public sector a customer (citizen) coming to a branch (counter) is always more expensive than solving the issue electronically. In March 2005, for example, Germany defined a federal eCard strategy requiring all smart-card-based projects to support digital signatures. With over 80 million citizen smart cards expected to be in use by 2008, Germany and the institutions participating in the program are expecting significant cost-cutting and efficiency benefits. A large pharma company has also reported savings of up to $100 per signature vs. managing signed paper documents. By introducing eID cards thus may profit not only public institutions, but also private companies [15].

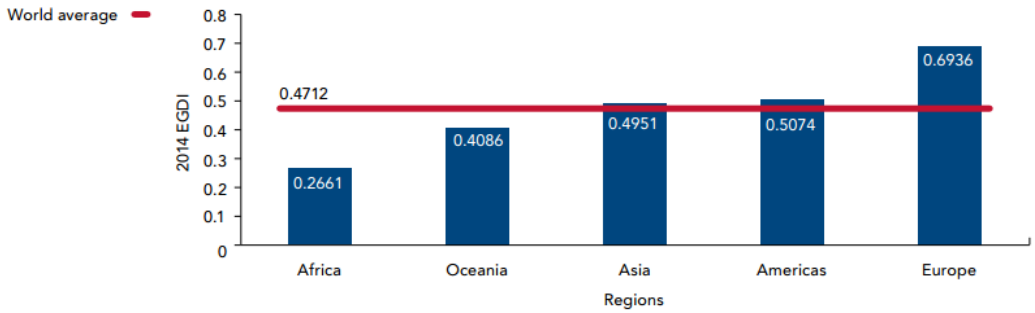
In a number of African countries, another area where trusted electronic identification may bring cost savings and making the whole process more efficient is issuing visa and other permits, such as hunting and fishing licenses. In Arkansas, permitting system has automated the process of applying for and awarding hunts on public land in the state. Around 55,000 permits are awarded each year to hunters, and 3,000 of those are sold in a one-time "left over sale" day prior to the start of hunting season. In Mississippi the online permit application was reduced from 7 pages to 4, resulting in 5 minutes saved by every hunter applying for a permit online [16].

In this regard, in the European Union has been stabilised the so-called basic list of e-Government services. 'Basic' refers to the 20 services (12 for citizens, 8 for businesses) used to benchmark the online availability of public services. These are: income taxes, job search, social security benefits, personal documents, car registration, building permissions, declaration to police, public libraries, certificates (such as birth or marriage certificate), enrolment in higher education, announcement of moving, health-related services (citizens), social contributions, corporate tax, VAT, company registration, statistical data, customs declaration, environment-related permits, public procurement (businesses). The selected basic services, extended by the e-Democracy tools (see below) have been taken over by the aforementioned UN benchmarking for its evaluation.

In addition to the above-mentioned services the verified ID shows a great potential also in the field of electronic democracy. In the presidential elections held in 2013 in the Czech Republic, where (among others) a group of min. 50 000 citizens could nominate its candidate, it turned out that some candidate sheets showed up to 23 per cent error rate, i.e. providing false information that the residents had filled into the sheets. Despite the fact that the electronic declaration of support to a chosen candidate was not possible, the high error rate shows the possibility of misusing such tools, where the electronic collection of signatures would save the time required to transfer the documents (not only to support a chosen candidate in presidential or other elections, but also during petitions or referenda) into electronic form and their subsequent control (including e.g. possible duplication). Among other examples of the use of trusted ID within the e-Democracy tools there are e.g. participatory budgets, where the citizens may decide where to allocate a portion of the public funds, e.g. does the city promote a new school, or a hospital? Similarly to non-state websites the trusted ID then finds its place in discussion fora, which, due to the need to include a real name, become much more to-the-point and free themselves from anonymous insults including the possible manifestations of xenophobia and racism.

A regular UN e-Government evaluation [17] uses the so-called four-stage model of online service development where stage 1 corresponds to emerging information services, stage 2 to enhanced information services, stage 3 to transactional services and stage 4 to connected services. Each stage demands a higher level of sophistication and, often, increased commitment of resources. To reach qualitatively higher phases (stage 3 a 4) of provision of electronic services often necessitates also electronic identification, whose absence frequently does not enable transactions to be carried out or the advantages of related services to be used. These services are then not only more comfortable and user-friendly for the public administration customers, i.e. citizens and businesses, but also bring time and thus also financial savings to public administration.

Chart 1: 2014 Regional Averages of e-Government Development



According to the last UN survey, Africa is the least advanced region in e-Government (see Chart 1), as the report states in more detail: „Progress remains relatively slow and uneven. *The regional EGDI average in Africa is 0.2661. Six countries (Tunisia, Mauritius, Egypt, Seychelles, Morocco and South Africa) have EGDI values above the world average of 0.4712, placing them among the top 50 % of the world. On the other hand, about 30 % (16 countries) of the 54 African countries are at the bottom 10 % of the world ranking"*[17] The introduction of trusted electronic identity and its integration into e-Government services could contribute to a significant improvement in the current state of affairs and to reduction of the digital divide. In this regard it is essential to point out that the situation in eIDs introduction cannot be generalised, but it needs to be analysed in each country individually, not as a continent as a whole. Some African countries such as South Africa or Nigeria have already introduced and started using successful identification tools, same as in Europe are countries (including the Czech Republic) in which the introduction of state eID tools is still waiting for its chance and the position of an eID provider is carried out by private sector, for example the mojeID service operated by the CZ.NIC association, the operator of the national domain .cz.

The case studies of countries as Denmark, Norway or New Zealand show that very good results in international e-Government ratings may be achieved even without eID and, moreover, without ID cards. In the 2014 UN e-Government Survey [17] these countries are among world e-government leaders. New Zealand came in 9th, Norway 13th and Denmark at 16th place.

6. Conclusions

Electronic identification represents one of the basic building blocks of e-Government. Trustworthy electronic identification offers great potential to public administration, as well as to private sector. Private sector can very well apply verified eID in a range of business cases, from e-shops to electronic banking to community services (such as carpooling). Trusted electronic identity can also fight the misuse of the Internet's anonymity, e.g. user ratings and reviews or discussion fora.

In Europe, as well as in the rest of the world, we can see various technical systems of electronic identification. Among the most widespread are chip cards that use qualified certificates and PKI. However, at least in terms of user-friendliness, this system has been partially overcome and countries such as Austria, Estonia or Iceland offer their citizens the possibility to use mobile eID. The citizens are often used to this system from electronic banking and they do not need such a high computer literacy level to use it. Given the experience with mobile payments and other application in Kenya and other African countries this solution seems to be the most suitable one. Besides mobile eID another example of a successful implementation of identification and authentication tool may be brought about by the cooperation with banks (or payment card issuers). In Africa such a model was chosen by Nigeria, where the Nigerian Identity Management Commission

(NIMC) has launched a pilot phase in 2014 and issues MasterCard-branded identity cards with electronic payments functionality. When it comes to the cooperation of the government and private sector, it is necessary to pay increased attention to protection of citizens´ personal data.

The possibility to use documents issued in one state in another country constitutes a specific electronic identification issue. While in the physical world it is commonplace, for the electronic world and e-identification this solution still represents a big challenge coming with a number of technical and legal obstacles. Europe currently plays the leading role in mutual recognition of eIDs, as since 2008 the STORK project has been demonstrating the advantages of cross-border identification when using both public and private services. In 2014, the adoption of eIDAS laid down the legal basis for cross-border identification, which will in 2018 make the interconnected services indispensable part of the Single Digital Market. This solution may serve as an example also for African states, e.g. within the African Union. The solution of STORK 2.0 is not limited to European states only but non-EU states may join as well, as was the case of the United Arab Emirates in December 2013. The STORK 2.0 solution for verified login of European users may be integrated in African countries too, e.g. in case of hunting permit applications.

References

[1] COM(2010)245
[2] COM(2010)743
[3] More information see www.eid-stork.eu
[4] More information see www.eid-stork2.eu
[5] More information see www.mojeid.cz
[6] STORK project authors; D 3.3.5 Smartcard eID Comparison; 2010; https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1384
[7] Press Release: “MasterCard-Branded National eID Card Launched in Nigeria”; http://newsroom.mastercard.com/press-releases/mastercard-branded-national-eid-card-launched-nigeria/
[8] Jackson, Tom; *Privacy International critical of Nigerian eID cards*; ITWebAfrica; http://www.itwebafrica.com/ict-and-governance/265-nigeria/234218-privacy-international-critical-of-nigerian-eid-cards
[9] Why does Kenya lead the world in mobile money?; The Economist; 27. May 2013;
[10] More information see https://www.digid.nl/index.php?id=1&L=1
[11] STORK 2.0: Added Value; https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=20&Itemid=48
[12] STORK 2.0 D3.2 – QAA Status Report https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175
[13] eIDAS Private Sector Engagement High Level Event "eID: a key to business growth and innovation"; Event summary from the view of the Commission; http://ec.europa.eu/digital-agenda/en/news/eidas-private-sector-engagement-high-level-event
[14] STORK 2.0: Work Overview; https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=30&Itemid=31
[15] Adobe Briefing Paper; *eID cards: Improving trust and reducing the cost of e-government transactions;* 2015;
[16] NIC International Company: Case Study 02: Hunting and Fishing; https://www.egov.com/what-we-do/case-studies/hunting-and-fishing
[17] ST/ESA/PAD/SER.E/188; United Nations e-Government Survey 2014; United Nations; New York, 2014;