Moldova Mobile e-ID solution

How mobile identification in the virtual world opens a gateway to public services in Moldova

Case Study

September, 2014 - PRELIMINARY DRAFT - for discussion only

Terms and Definitions

Authentication - The process of identification of the user in a given information system;

Authorization - The process of determining user's rights in a given information system;

CA – Certification Authority;

CTS - Center of Special Telecommunications – Moldovan state enterprise;

DS - Digital Signature;

Electronic identity - a collection of identity attributes in an electronic form;

HSM - Hardware Security Module;

MCloud - Moldova's electronic services delivery platform based on cloud computing;

MPass - Governmental Identity Service based on national identification number as username and password;

MSign – Governmental Signature Service offering centralized signing functionality for e-services;

PKI - Public Key Infrastructure;

RA – Registration Authority;

Signatory - the person who applies digital signature to electronic content;

Signature Directive - Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures;

SIM - Subscriber Identity Module;

SSCD - Secure Signature Creation Device;

WPKI - Wireless Public Key Infrastructure

INTRODUCTION

In 2011, the government of Moldova embarked on a strategic program for public service and governance modernization. Once the government created the Council of e-Transformation Coordinators in ministries, agencies and all other central public authorities, and established the e-Government Center within the State Chancellery, the World Bank approved the $20 million IDA credit aiming to support the implementation of the *Governance e-Transformation* (GeT) project. The key project development objective was to radically transform delivery of public services using information and communications technologies (ICTs).

Implementing this ambitious program entailed a complex reform of 587 public services for citizens and businesses, including evaluation of quality standards indicators, new methodology for public services' tariffs, the registry of public services and the introduction of e-Government practices and tools, with the aim of cutting bureaucracy, corruption, administrative costs, inefficiency and low levels of productivity.

A bold undertaking of the GeT project was the deployment of the mobile eID infrastructure (MeID), which is critical to the delivery of public services. The MeID platform aimed to enable the speed, the privacy, the convenience and transparency of digital access to numerous government services and information for citizens, including online applications and copies of official documents.

In 2012, the government of Moldova, in partnership with leading telecom operators, launched the *Mobile Signature* service. This was one of the first and most successful MeID public-private partnerships (PPPs) in the world. At international level, such an authentication service via the mobile phone is only available in six other countries. At Mobile World Congress 2013 in Barcelona, the government of Moldova received the *m-Government Global Mobile Award* from the GSMA for the *Mobile Signature* project.

MOBILE ID SOLUTION DESCRIPTION

The *Mobile Signature* works as an ID in the virtual world, allowing users to authenticate themselves in the cyberspace in order to prove their identity with the cellphone. In Moldova, this solution for citizens' identification and authentication on the mobile platform requires replacing the regular SIM card of the cellphone with a special SIM card that includes the functionality to produce digital signatures using

mobile phone. Citizens can easily obtain the mobile signature from mobile operators. For this they have to take their current ID card to the mobile operator and complete an application form, the whole process taking less than 15 minutes. The process of accessing public services using MeID is also very simple. The detailed usage scenario and access to the public services portal **servicii.gov.md** with the MeID is described in the **Figure 1** below.

Figure 1 : Usage scenario for MeID

Source: e-Government Center, government of Moldova

EVIDENCE OF RESULTS & KEY SUCCESS FACTORS

Results start to be visible, despite recent launch of the platform. High exposure public services provided to business through online channels have been streamlined and taken up due to use of MeID. About 50% of businesses reporting to National House of Social Insurance use MeID on a regular basis. There is a growing trend for adoption of MeID by citizens as well. Roughly 40% of all digital signatures applied by citizens to the electronic services accessed are mobile signatures. The trend is

positive, adding on average 0.3% to 0.5% to the above-mentioned volume every month.

Integration of e-services with the MeID and electronic payment MPay platform proved to be highly beneficial and contributed to the uptake of ICTs in Moldova. Overall, public sector applications are driving uptake, while private sector applications are driving scale.

The success of the MeID service is undoubtedly due to a strong partnership that has been established between the state agencies and the private sector operators. In addition, the participating mobile operators - competitors on the Moldovan market - did not compete on MeID functionalities, but rather on the quality of service provided. Currently, the mobile penetration in Moldova exceeds 100%, and there are more than 3 million subscribers to mobile services.

Other key success factors are :

(i) Strong championship of the State Chancellery and sustained capacity development efforts within government agencies
(ii) Knowledge sharing activities facilitated by the World Bank (IDM Experts Group[1]) and other development partners
(iii) Reuse of the existing infrastructure (e.g. PKI)
(iv) Use of proven technologies and standards
(v) Existence of enabling environment and favorable regulatory framework

PROJECT PREPARATION

In preparing the MeID project, the government of Moldova paid a particular attention to the fact that it fits well with the overall e-Government program and the objectives of the GeT project.

The Strategic Program for Governance and Technological Modernization, approved in September 2011 and the overall Framework for Identity Management, developed by the government, provided the right legal and regulatory environment that enabled

[1] Identity Management (IDM) Experts Group – a bold undertaking of the World Bank who in association with a number of partners is creating a global network of experts to broker knowledge and provide quick access to cutting-edge expertise in the area of identification. The overall purpose of the initiative is to help governments in developing countries to design and implement projects aimed at strengthening the delivery and quality of public services, using modern identity management tools.

project preparation. According to the July 2004 law, electronic documents in Moldova are equivalent to paper-based documents signed by hand. In September 2012, the Prime Minister issued a government ordonnance that legalized the MeID solution as part of the electronic services provided to the citizens of Moldova.

Prior to developing the solution, the government of Moldova undertook an extensive analysis of the options available. The World Bank has facilitated access to cutting-edge expertise in this area, namely through consultations with the IDM Experts group (detailed analysis, including costing, along with the recommendations made by the experts group, are presented in the **Annexes**).

A summary of the key criteria considered by the government and the critical questions/issues that had to be addressed when designing the MeID solution, are presented in **Table 1** below.

Table 1 : Elements of analysis in the design phase of the MeID solution

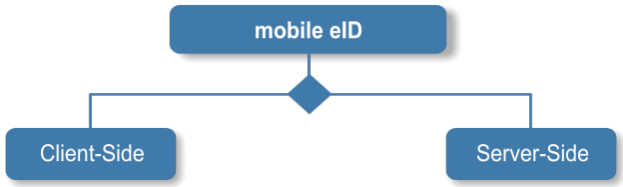
#	Key criteria considered	Key questions asked
1.	Cost of implementation	How much it will cost the state to implement the system?
2.	Cost of maintenance	How much the state will have to pay yearly to keep the system operating?
3.	Implementation timeframe	How long it will take to implement the system? When it could be potentially launched?
4.	End user uptake: -> usability	How comfortable will the end users be with the new system? -How easy it will be to issue a DS kit? -How easy it will be to extend/replace the certificate after expiration of its validity period? -How easy it will be to use the DS with the model?
5.	End user uptake: -> costs	How much it will cost users using this model: -How much will they have to pay for registration/activation? -How much will they have to pay for regular service provision? -What are indirect costs they would have to support (i.e. buying a new cellphone because the old one is not suitable for the DS model)?
6.	Administrative usability	How easy it will be to administer the process of: -Issuing a DS; -Mapping to the natural person; -Revoking a certificate; -Extending/replacing a certificate
7.	Technical support	How the users will be supported in using DS? Who will offer that support?

In addition to the above, the government of Moldova had to develop and implement identity management and authentication standards and tools that:

- uniquely identify users and offer highest level of security known as of today;
- are highly re-usable, has low total cost of ownership and could be implemented and launched in short timeframe;
- are accessible to every citizen and business of any size.

In the end, the government had to chose from two alternatives, each with its specificities, presented in **Figure 2** below.

Figure 2 : the MeID alternatives considered



Using special SIM cards with PKI functionality that enable the SIM card's owner to carry out signatures "on-board" the mobile device by using the SIM card as cryptographic device, the handset for PIN entry and the mobile operator's network as backchannel.

No electronic signatures have to be carried out on the phone itself. The cell phone solely acts as an second authentication channel receiving TANs via SMS. This certificates are stored using HSM and are accessible only by using PIN.

Source: e-Government Center, government of Moldova

In the client-side MeID option, the cryptographic material is stored on the client (i.e. on user's mobile phone) and the mobile subscriber is provided with a special SIM card which contains the PKI functionality. In the server-side MeID option, the cryptographic material is stored securely on a Hardware Security Module on the server and no SIM replacement is required. Both options are compliant with EU legislation on digital signatures, namely the EU Directive 1999/93. The client-side MeID is implemented in several countries, including Estonia, Finland and Sweden, while the server-side MeID is implemented by the Austrian federal government.

After a thorough analysis conducted, the government chose to deploy the client-side MeID option. It has subsequently put in place robust M&E tools for evaluating MeID usage and uptake, which are made public on a monthly basis. On the technical level,

the government is monitoring the performance of MeID service, as part of the government PKI infrastructure evaluation process.

PROJECT IMPLEMENTATION

Unlike other countries where the development of mobile identification and authentication services was dictated by the banking environment, in Moldova the MeID service deployment was realized thanks to the partnership between the government and the private sector. This in itself is a good indicator of cooperative, open and transparent governance. A detailed description of the implementation arrangements and roles' distribution is presented in **Table 2** below.

Table 2. Implementation arrangements/Roles' distribution

	Government	Mobile Operators	
Enrolment	CA Role Issue qualified signature certificates	RA Role Ensure large coverage through distribution network	ESP (Gvt/Private)
Operation	Role - Validation - Time stamping	Role Provides end-user operation and secure data exchange with CA: - Signature on handset - End user charging - Customer support	Role -Consumes Mobile Signature Services

Moldova faced no significant delays in implementing the MeID solution, certainly due to strong commitment of the government team to deliver the project and the speed and commitment of the mobile technology companies. Since the major part of the investment required in infrastructure procurement was provided by the private partners (mobile operators and vendors), the State Chancellery didn't have to conduct additional procurement for the MeID implementation. Instead, it built on the existing PKI government infrastructure and let the private sector chose and procure what was mostly appropriate for a reliable, cost-efficient and rapid MeID platform deployment. The Gemalto UICC-based technology was chosen by the private partners/mobile operators since it was compatible with all types of mobile telephones used in Moldova. The technology allows citizens to confirm their identity and sign documents directly from their mobile phone, by entering a unique user-selectable PIN code. The embedded Valimo Mobile ID application transforms any

type of mobile phones into devices capable of delivering strong user authentication and legally binding signatures, essential features to securing e-Government services.

LESSONS LEARNED

Past experience in comparable contexts has demonstrated that low adoption of the traditional digital signature solutions is mainly due to the:

- lack/limited number of e-services provided to citizen
- insufficient mobility – card readers needing to be carried and additional client-side software needing to be installed on client computer
- insufficient portability – classic digital signature kits on smartcards being impractical on new platforms, such as tablets
- insufficient outreach – existence of a single registration authority in the capital city
- insufficient client support – lack of capacity to offer high quality client support
- high costs associated with the deployment and usage of infrastructure

Accordingly, an operating model responding to the above-mentioned challenges was developed to ensure:

- large scale deployment capability
- multi-dimensional adoption of services (both governmental and commercial)
- collaborative promotion and client support
- financial sustainability of the deployment and operations

Another important challenge that has to be addressed is the privacy/personal data protection. To ensure that MeID is implemented in accordance to the personal data law, the government strengthened the National Center for Personal Data Protection and has launched the Register of personal data operators. This registry is an information system that contains records of all personal data controllers who've accessed personal information of citizens. This in turn enables citizens to find out exactly what entities/operators are processing their personal data and for what purposes.

The government is convinced that the best guarantor of MeID service sustainability is the partnership with the mobile operators, in a context of clear repartition of roles and responsibilities and a healthy business model in place. The later is a PPP based on revenue sharing. The partnerships agreement provides for mobile operators to define the conditions of the MeID use, including the costs for the mid and long term cost recovery.

The initial challenge of convincing the private sector to enter into such a partnership with the government was addressed through high-level political commitment and support from the World Bank. To affirm its long-term vision, the government made it mandatory for all public services provided online to be integrated with MeID platform through MPass and MSign and is actively supporting this integration.

Successful implementation of MeID in collaboration with mobile operators served as a good and encouraging example of government/public entities partnering with the private sector. Additional infrastructures have been/are being implemented following this model. In September 2013, the Government launched the electronic payment service – MPay which makes it possible to pay for any (participating) public service with any payment tool legally functioning in the country. As of today, all commercial banks (14), all cash-in networks (3) and all post offices (over 1000) are part of the electronic payment infrastructure. Currently the government is working on mobile payments based on digitally signed electronic invoices using the mobile signature service. Thus, MeID is truly opening a gateway to public services in Moldova.

Cost analysis for the MeID solution for the public sector in Moldova

INTRODUCTION

One of the key components of the e-Government technology platform is the Authentication and Access Control service. The authentication part of this service is based on the Provider architectural pattern and will offer several authentication mechanisms. One of the envisioned ways of authenticating users is through mobile devices. On June 1st the e-Government Center presented to the public a concept note describing the envisioned approach to mobile eID. That note was describing two alternatives of implementing mobile eID – client side implementation, when user's qualified digital certificates are stored in the SIM and server side, when the certificates are stored in a remote and secure hardware module. One of the goals of the public consultations was to collect enough feedback to be able to decide on which alternatives to implement for the public sector. The consultations shown that the community is interested in mobile eID service, still the cost analysis shall be conducted in order to understand how much the state may spend on this service.
This document describes the components forming the cost for the mobile eID solution as well as final costs identified during analysis.

CURRENT STATUS

Public consultations on mobile eID showed high interest in such service in both public and private sectors. Most of the feedback confirmed that this technology would solve the deficiencies current eID has, especially high costs and reduced usability.

To conclude public consultations the working group had a series of summarizing sessions. Based on identified criteria and on feedback collected during consultations the group compiled the summary Table 1 below. The table contains the list of criteria; their weights as given by the group, the score given by the group to each criterion (scale 0…10) as well as accumulated points resulted from multiplication of the score and the weight. The final result showed a minor difference (~8%) in the accumulated number of points, demonstrating that both solutions are perceived as being of roughly similar value.

Table 1 : summary of scores given to each solution during experts' consultations

#	Criteria	Weight	client		server	
			score	points	score	points
1	Implementation costs	7	7	49	9	63
2	Operational costs	9	9	81	7	63
3	Implementation time	5	5	25	9	45
4	Usability	10	8	80	9	90
5	Cost for citizen	8	7	56	9	72
6	Ease of administration	1	8	8	9	9
7	Customer support	9	8	72	8	72
8	Private sector uptake	7	9	63	7	49
9	Security	10	9	90	7	70
10	Reliability	9	8	72	9	81
11	Neutrality	9	5	45	9	81
	Total points:			**641**		**695**

As a next step it was decided to perform a more detailed cost analysis. The working group has collected data regarding costs for both options. Based on information provided by implementers of client-side mobile eID in Estonia, the cost of implementation for the client side is cca. €300 000 for each mobile operator participating in the mobile eID infrastructure. To this amount it should be added the costs for components which are common for all operators. Based on information from implementers of Austrian mobile eID solution the cost for server side option is cca. €350 000.

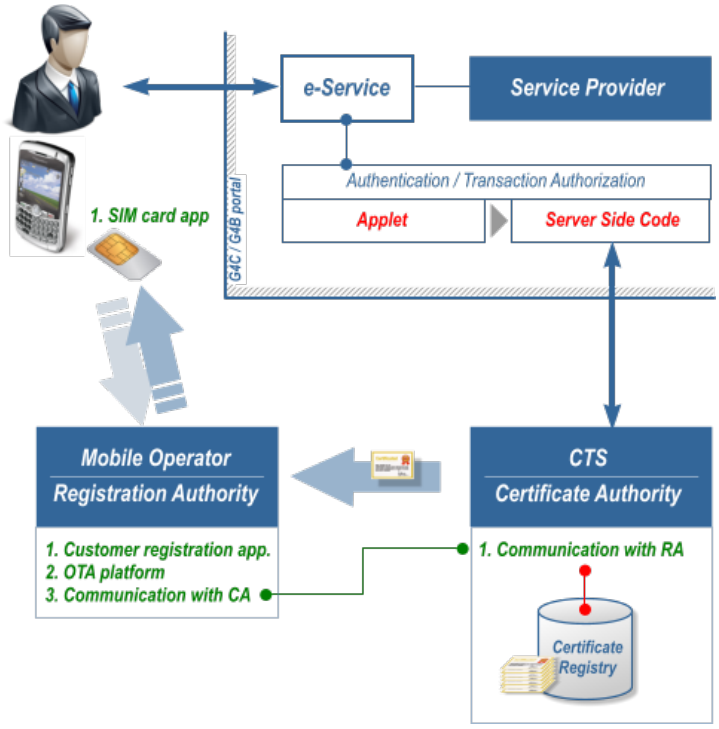
The sections below give a high level description of the components which generate these costs.

CLIENT SIDE MOBILE EID PLATFORM

The platform for the client side mobile eID solution has the following players:

1. Certificate Authority (CA) – this role is assigned to CTS, which is the level 2 CA in the national PKI;
2. Mobile Operator/Registration Authority – this role is played by a mobile operator;
3. Service Provider – this is the organization offering electronic services through G4C/G4B portal;
4. Client – the citizen accessing electronic service offered by service provider.

The diagram below illustrates the players as well as their associated hardware and software components.



The components which shall be deployed at and/or operated by the mobile operator are the following:

1. SIM card application – the application embedded into the secure area of the SIM card used for digital signing. This means that current SIM cards will be replaced with new ones using mobile operator customer service network.
2. Customer registration application – the application which keeps records about clients with PKI enabled SIMs.
3. OTA platform – hardware plus software solution which ensures communication with WPKI enabled SIMs using other the air protocols.
4. Communication with CA/TSP – the application which ensures communication with CA/TSP, which in particular sends signed data back to the TSP to be sent to the SP.
5. Communication with RA – the application which is deployed at the TSP site and is responsible for the communication with RA, in particular for sending date to be signed to the PKI module.

The components which are developed and operated by the state are the following:

1. Mobile eID applet – an web page applet, which is responsible for receiving user's phone number and displaying transaction verification code, which derives from data to be signed.
2. Server side code – the server side code which takes the information from the applet and passes it to the TSP along with data which has to be signed.

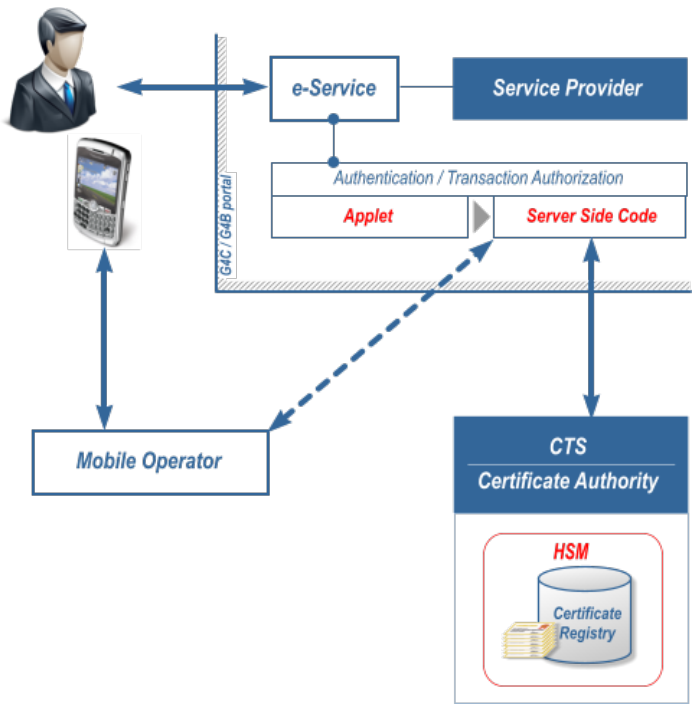
If implemented at the portal level, then both the applet and the server side code could be re-used by e-services within C4C/G4B portal.
Apart from above mentioned component an additional integration task should be performed – communication between the CA↔RA application and certificate registry of the CA.

SERVER SIDE MOBILE EID PLATFORM

The platform for the server side mobile eID solution has the same actors, however the responsibilities within the authentication and signature process is different, therefore the investment distribution is different too:

1. Certificate Authority (CA) – this role is assigned to CTS, which is the level 2 CA in the national PKI;
2. Mobile Operator – this role is played by a mobile operator;
3. Service Provider – this is the organization offering electronic services through G4C/G4B portal;
4. Client – the citizen accessing electronic service offered by service provider.

The diagram below illustrates the players as well as their associated hardware and software components.



The components which shall be deployed are the following:

1. A-Trust Security Module – an appliance consisting of a specialized safe with embedded Hardware Security Module (HSM).
2. Mobile eID applet – a web page component, which is responsible for receiving user's phone number and displaying transaction verification code, which derives from data to be signed;
3. Server-side code – the server-side code which takes the information from the applet and communicate it to HSM along with data which has to be signed.

In this architecture there are no components hosted or operated by mobile services provider. The system would use only transport capacity of mobile operators' networks.
If implemented at the portal level, then both the applet and the server side code could be re-used by e-services within C4C/G4B portal.
Apart from above mentioned component an additional integration or migration task should be performed which should ensure data exchange between HSM and existing certificate registry of the CA.

COST ANALYSIS

The cost of the overall solution consists of costs for each and every component presented in the above infrastructure, the integration and testing activities, as well as operational costs.
There is a direct relation between the cost of the solution and the cost each and every user will have to support. Major government concerns in regards to costs and efficiency of the mobile eID solution are:

1. What are the costs for the state to implement and launch the system;
2. What are the operational costs of the system the state will have to support;
3. What is the price for the service citizens will have to pay;
4. What is the implementation timeline – how fast the service can be launched;
5. Is the solution future proof, is it extensible.

IMPLEMENTATION COSTS

Client-side

Preliminary estimates show that the overall costs of the solution are cca. €400 000.
In an eventual private public partnership, the state part could be the PKI infrastructure, costs of implementation of common/generic modules, i.e. modules which are not dependent on mobile operator and integration works in the CA side (assets colored in red on the client-side diagram above). These costs are evaluated at cca. €100 000. The operator contribution will be the implementation of specific components, such as OTA platform, customer registration system etc. as well as the costs of replacing old SIM cards with new ones with PKI unctionality (assets colored in green on the diagram). These costs are evaluated at cca. €300 000 for each operator.

Server-side

The implementation costs of the server side solution is evaluated (by A-Trust from Austria) at €350 000. In case of server-side implementation this cost would have to be covered entirely by the state.

OPERATIONAL COSTS

Client-side

Operational costs for the government will consist of costs to maintain the PKI infrastructure (under the process of estimation by the Government).
Operator will have to evaluate its operational costs.

Server-side

Operational costs for the government will consist of costs to maintain both mobile eID and the PKI infrastructure (under the process of estimation by the Government).

COSTS FOR THE CITIZEN

Client-side

Preliminary analysis shows an indicative registration price of **€4**. This price covers the replacement of new SIM card (€3) and the qualified digital certificate issued by CA (€1).
During business as usual, a flow of SMS messages between citizen and RA will take place.
There are two options to cover the cost of these messages by:

- Applying a constant monthly fee, which is evaluated by operators at **€1** per month. In this case the return of investment depends on number of users subscribed to mobile eID services.
- Paying for exact number of messages sent and received during the process of authentication and digital signing. In this case the return of investment depends of number of actual transactions performed by subscribers.

During working sessions with operators it was clearly stated that the costs supported by citizens are those which recover the costs and will directly influence the profitability of the project. The operators would accept to invest in the service and to cover all the costs on their side (estimated at €300 000) if the Government is determined to develop and implement a rich portfolio of e-services for citizens and business on ongoing basis and enable through different types of incentives and advocacy campaigns the uptake/usage of the e-services.

Server-side

Since the server-side solution is own and operated entirely by the state, the Government could be flexible with pricing policy for mobile eID services. In particular, in order to incentivize citizens to use mobile eID the registration fees could be symbolic or excluded at all.

However, the there are some expenses related to SMS communication which should be supported by citizens. The Government could negotiate with mobile operators acceptable volume prices for this particular type of messages.

IMPLEMENTATION TIMEFRAME

Client-side

Analysis shows that client side mobile eID can be implemented in 5-6 months. This is an acceptable timeframe and is in line with other dependent and planned deliveries. However the process of replacement of SIM cards may take up to 24 months.

Server-side

Implementation timeframe for the server-side option is estimates at 3-4 months.

SOLUTION EXTENSIBILITY

An important aspect is the extensibility of the solution, since the extensibility in this case protect the investment. For example, if the state will decide to implement authentication using biometric data, then the mobile eID infrastructure will be capable to handle it with little or no additional investment.

Client-side

The analysis shows that the solution is extensible since modern SIM integrated circuits have sufficient capacity to store additional data such as citizen biometry. In addition, since the evolution of mobile devices is very dynamic, it is possible that the PKI functionality on client side could be a part of other scenarios.

Server-side

The server-side solution also offers sufficient extensibility, since the main processing happens on the server. In this case there are no technical constraints pertinent to mobile devices.

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS:

1. Both solutions satisfy public sector needs.
2. Although total implementation cost for client-side is ~15% higher than the server-side, in case of a partnership between the Government of Moldova and mobile operators these costs could be split and the sustainability model could be ensured..
3. Operational costs from state prospective for both solutions are nearly the same.
4. The costs for citizen in case of client-side is higher, however they are incomparable with current costs for eID.
5. Both solution are sufficiently extensible and offer attractive prospects for development.

RECOMMENDATIONS

The working group makes the following recommendations, based on its commitment to define the best solution that would respond to citizens and Government needs, and contribute to an enabling business ecosystem for the private sector.

1. Although server-side implementation satisfies public sector needs, the working group recommends to investigate the possibility of public private partnership with mobile operators and to implement client-side solution. The main reasons would be:
    a. Existing interest from private sector/mobile operators;
    b. Possibility to use operators' distribution networks for issuing certificates;
    c. Perceived security of client-side is higher than of server –side;
    d. Better promotion of mobile eID services using operators' capacity;
2. The working group recommends to evaluate the price for the citizen (registration, monthly or per-sms fee) deriving from more accurate projection of number of users and transactions.
3. The working group suggests using prices for each SMS instead of applying a constant monthly fee. In our opinion this is a better model for the short term.

REFERENCES

1. Concept Note on Authentication and Mobile Electronic Identity, e-Government Center, June 2011, [http://egov.md/upload/CN-mobile-eID-eGC-June-2011-ro.pdf]