June 1st, 2011

CONCEPT NOTE

Authentication and Mobile EID for the Public Sector in Moldova

Introduction

The Government of Moldova, as part of its e-transformation initiatives, is building a shared infrastructure – a new e-government technology platform using modern technologies such as cloud computing and offering multichannel access to information including access from mobile devices. At the Platform as a Service level, this environment has several shared services which are also known as enabling services since their successful implementation and operation will give a significant impetus to the development and usage of e-services. One of these enabling services is the Authentication and Access Control (AAC) service. This service will implement basic security tasks such as identifying and authenticating users, authorizing their transactions and determining their rights into various governmental information systems. This paper describes in details the current situation as of May 2011 and the options for implementing the AAC service.

Terms and Definitions

Authentication	-	The process of identification of the user in an information system;
Authorization	-	The process of determining user's rights in an information system;
CRM	-	Customer Relationship Management (system);
CTS	-	Center of Special Telecommunications;
DS	-	Digital Signature;
Electronic identity	-	a collection of identity attributes in an electronic form (European Union STORK definition);
ESB	-	Enterprise Service Bus
G4B	-	Government for Business (portal);
G4C	-	Government for Citizen (portal);
GIS	-	Geographical Information System;
HSM	-	Hardware Security Module;
M-Cloud	-	Moldova's electronic services delivery platform based on cloud computing;
Mobile Identity	-	portable electronic identity;
M-Pass	-	National Authentication Provider based on national identification number as username and password;
M-Point	-	A kiosk installed in every location in Moldova providing access to e-services;
PKI	-	Public Key Infrastructure;
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, published in the Official Journal of the European Communities (OJ) L 13, 19.01.2000, p. 12.
SIM	-	Subscriber Identity Module;
SLA	-	Service Level Agreement;
SSCD	-	Secure Signature Creation Device;
WPKI	-	Wireless Public Key Infrastructure

Platform architecture

As part of the e-Government technology platform, Moldova is going to build a new shared infrastructure which will allow ministries and agencies to host information systems within it. This infrastructure will be built using cloud computing – a promising modern technology which changes the delivery of IT services into an efficient self-service provision of IT resources combined with pay per use models. For convenience purposes, in Moldova, this cloud computing technology will be called M-Cloud.

This platform is in essence a private cloud offering three main service delivery models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

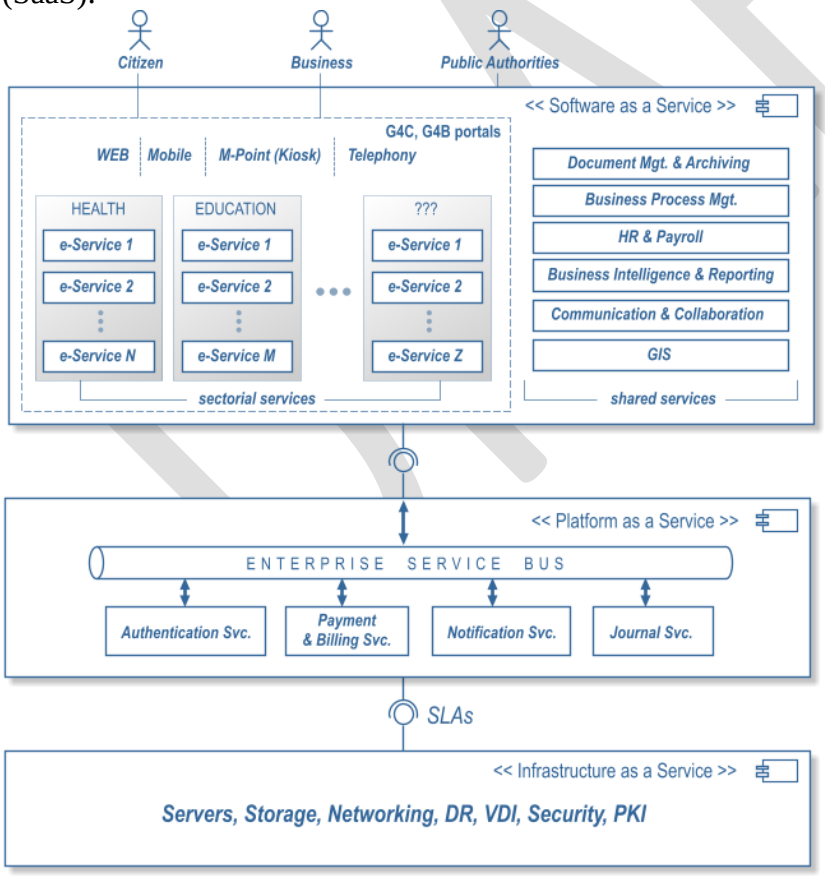

Fig. 1. The high level architecture of the e-government technology platform

The Infrastructure level services will mainly rely on re-using existing and upgraded service provision offered by CTS. Using these services will allow ministries and agencies to extend

their IT capacity in a very short time frame. When requested resources are no longer necessary, the agency will be able to scale them down, therefore functioning on a pay-for-usage basis.

The Platform level services will offer common functionalities to business services operated by ministries and agencies on the Software as a Service level. At the time being, the architecture defines four re-usable Platform level services:

- Authentication and Access Control service (AAC) – provides a unified way to solve application security related tasks such as identity management, authentication, transaction authorization etc.;
- Payment service - provides a unified way to implement electronic payments;
- Notification service – provides an unified way to send notifications when needed, thus allowing for offline interaction with citizens;
- Journal service – provides a unified way to store and retrieve data regarding users activity within information systems.

Platform level services are intended to be utilized by current and future electronic services that ministries and agencies can develop.

The M-Cloud platform also contains a communication layer based on an enterprise service bus (ESB). Through this bus, services will be able to exchange messages. This in turn will allow creating complex business processes that are to be orchestrated by business process management tools.

Services delivered at the SaaS level could be grouped into two major categories – sectorial services and shared services.

Sectorial services are implemented and maintained by different sectors, such as education, healthcare, social protection etc. and directly consumed by citizens. These services are accessible through a common portal. Access to the portal will be possible through different channels such as web, mobile or kiosks, with the later being called M-Points, for convenience purposes.

Shared services at the SaaS level are those services which will be used across ministries and agencies. Examples of such services could be electronic document management system, human resources and payroll system, CRM and reporting system etc., i.e. those services which help optimize the work of public sector authorities.

Platform level services design

Since platform level services will be re-used by many business services in a multitude of contexts, they should be highly configurable to accommodate different usage scenarios. On the other hand, several companies expressed their interest in providing commercial solutions.
The architecture of platform level services will be based on provider architectural pattern, which decouples the generic service from its specific implementation. In this case vendors will have to conform to clear communication interfaces which act as technical contracts between components.

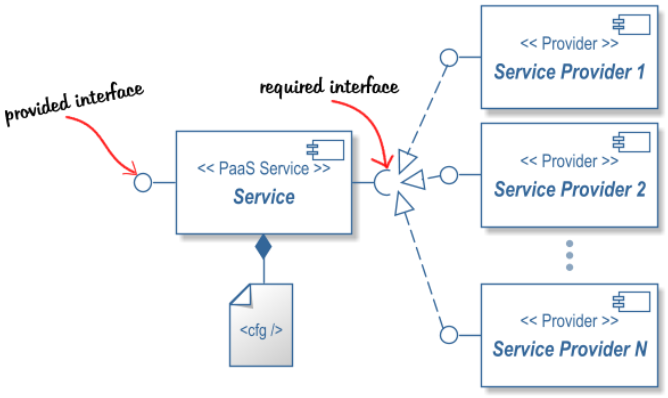

Fig. 2 The provider design pattern

Translated to authentication, the provider model would look as in the diagram below.

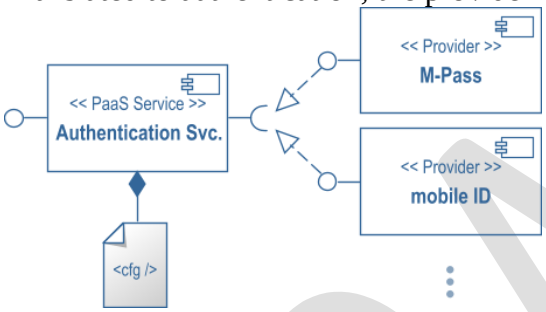

Fig. 3 Provider model applied to authentication

According to this design, different authentication/authorization providers should be integrated into the architecture. For the time being we have identified two providers: M-Pass and m-ID. M-Pass is an authentication provider which accepts user's credentials, namely username and password and as a result issues an authentication ticket in case of successful authentication. M-Id is another provider which authenticates users and authorizes transactions based on digital certificates issued by the national certificate authority.
This provider model offers higher flexibility accommodating different usage scenarios. For instance, certain services might use M-Pass while other services that demand a higher level of security might use m-ID, Also within the same service, authentication could use M-Pass while some transaction authorizations may use m-Id. Although exceptions are admitted, the general rule is that one way communication services (i.e. server presenting some information to users) will use simple authentication using M-Pass, while for two way transactional communication services will use mobile eID.

Mobile identification

We analyzed several implementations of electronic and mobile identity in several European countries which comply with the European Parliament Directive 1999/93 on a Community framework for electronic signatures, published in the Official Journal of the European Communities (OJ) L 13, 19.01.2000, page 12.
This directive states that EU member countries had to implement and widely use electronic identity by mid 2001. Even now, after a decade the high expectations concerning usage and uptake of qualified electronic signatures could not be met. This is somehow puzzling since on

one hand we have high and constantly growing number of phishing attacks and identity theft[1] while on the other hand, we have the low adoption of qualified electronic signatures, although this is a perfectly adequate answer to mentioned challenges.

Qualified electronic signatures are advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device.[2] Usually, the latter implies the usage of a specific smart-card. As off-the-shelf PCs and notebooks do not contain a readers for the simple use of a smart-card, the procedure required before the card can actually be used, can be quite time-consuming and costly. Besides requiring a formal registration procedure for identifying the signatory[3], the signatory has to buy a specific hardware component (smart-card reader), which may complicate the user experience and accessibility as this product is not generally available in shopping centres. Furthermore, additional installation procedures may be necessary for the card reader as well as the installation of software components for the signature applications. Furthermore, many applications involved may not be self-explanatory thus causing additional barriers for widespread usage.

Today there are various technical and organizational approaches for how mobile devices may serve as means for authentication. After the performed analysis we converged to two main valid alternatives of implementing this technology: a) client side implementation, where cryptographic material is stored in Subscriber Identity Module (SIM) located in client's mobile devices (the model currently used in Estonia) and b) server side, when cryptographic material is stored on the server in a Hardware Security Module (HSM) (the model currently used in Austria). Below is a short description of these alternatives.

Client side mobile identification

One approach for the realization of mobile electronic identification is to perform digital signature directly on the phone, using built-in secure elements, secure elements on special SIM cards or secure elements implemented on external hardware plugged in the handset.
The private key needed to conduct signatures is securely stored within such secure elements. Its usage is protected by a PIN known only to the holder of the phone so that the holder has the exclusive control over her/his credentials. The result of a digital signature is usually transferred to a communication partner, either using a GSM channel or some other communication technology like RFID, NFC or Bluetooth.

An already approved solution is the integration of a PKI module within a Subscriber Identity Module (SIM). This approach seems obvious since SIM cards are already installed and integrated in the phone, the distribution is ensured by the mobile operator and private keys can be generated on-card, so that they never leave the secure environment.

A SIM is a module that securely stores network specific information used to identify and authenticate subscribers on the Network, e.g.:

- like every smart card, a SIM provides a so called "Integrated Circuit Card ID" (ICCID), an international unique identifier,

[1] For interesting facts and figures see e.g. http://www.enisa.europa.eu/act/ar/deliverables/2010/preventing-identity-theft_training-material/at_download/file or the internet security threat reports by Symantec, http://www.symantec.com/business/theme.jsp?themeid=threatreport.
[2] Art. 5 para 1 of the Directive.
[3] See in particular Annex II d.) of the Directive.

- the International Mobile Subscriber Identity (IMSI), a unique identifier used by individual operator networks and
- an authentication key used to authenticate the SIM on the mobile network

Each subscriber is uniquely linked to the SIM which stores the user's private key needed for authentication based on signatures in tamperproof manner.
A SIM card in a phone can be regarded as a smart card fully integrated with reader and display in combination with networking functions.
The processes of registration, authentication or signing may differ from case to case, as outlined below:.

User registration process

1. The user gets a WPKI capable SIM card from the mobile operator.
2. If there are already private keys stored on the card, the PKCS#10 files and the public device certificates are already stored at the mobile operator.
3. The registration/certification authority (RA/CA) verifies the user's identity (not in scope of WPKI) and sends an activation code to the user.
4. The user contacts the RA/CA to start the activation process. Depending on the phone number the RA/CA identifies the appropriate mobile operator.
5. The RA/CA contacts the mobile operator via WPKI interface in order to start the activation process. The mobile operator checks if the user's SIM card has already pre-distributed keys included. If not, a special command is sent to the user's SIM card in order to start an on-board key generation process which involves the definition of the PIN codes.
6. The RA/CA receives the device certificate.
7. The RA/CA sends a signature request through the mobile operator to the user's SIM card.
8. The user is asked to enter the activation code which he additionally has to sign using his PIN code.
9. The signed code is returned to the RA/CA through the mobile operator.
10. The RA/CA verifies the signature and the activation code.
11. The RA/CA receives the PKCS#10 requests from the mobile operator.
12. The RA/CA generates the user certificates.
13. The user is informed upon the successful activation process.

Authentication process

1. The user wants to authenticate against a relying party. The relying party asks him for his phone number. The user enters his phone number.
2. The relying party performs a lookup by contacting each trusted registration/certification authority (RA/CA) via the WPKI search interface. If there are multiple search results (the user may be registered at several RA/CAs) for a given phone number the user has to choose a RA/CA.
3. The relying party displays the information to be signed on the "information channel" (the user's browser for instance) including the instruction that the user should sign

using the security channel (his cell phone). An optional control code may also be displayed.
4. The user's SIM card receives a signature request.
5. If a control code was used, the user has to enter the particular control code on the mobile phone. The user signs the displayed text by entering the PIN.
6. The mobile operator sends the signed message to the relying party which performs signature verification as well as a certificate validation sending an OCSP request to the RA/CA.
7. The RA/CA returns the certificate status.

Signing process

1. The user wants to use a service that needs authentication.
2. The user enters the number of his cell phone into the web form of the service he wants to authenticate against.
3. The cell phone receives an especially prepared SMS message from the service provider containing the text to be signed.
4. The user counter-checks the message text.
5. The user signs the message by entering his 4-digit PIN.
6. The message is signed using the SIM's PKCS#1 functionality.
7. The signed message is sent back together with the SIM's unique ICCID.
8. The verifying authority checks the signature. The certificate containing the public key needed to verify the signature may be retrieved by means of the ICCID transmitted by the signer.
9. The user is now authenticated upon the service provider.

Server side mobile identification

This innovative approach, which was presented to the public in the framework of the E-Government Ministerial Conference in Malmö end of 2009, enables qualified electronic signatures without additional software installation and hardware such as smart-card readers.
In contrast to client side "mobile eID" solutions, the server side mobile phone signature is not based on specific SIM-cards as the signature-creation data is stored remotely. Thus it is not the mobile phone itself holding the secure-signature-creation device required for qualified electronic signatures but a remote HSM. In the server side model, any mobile phone on any mobile operator network can be used, as it does not requirea specific SIM card and therefore does not require the user to change previous SIM-card. The only technical requirement is for the mobile phone to be able to send and receive SMS.

Similar to many solutions used by banks for e-banking purposes, after typing the phone number (as user ID) and password, the user receives an SMS to the registered mobile phone containing a one-time ephemeral code (TAN). Entering this TAN, a qualified electronic signature is triggered using a qualified certificate and signature-creation data stored in a hardware security module (HSM) securely held by the provider.

User registration process

The technical process for generation of signature-creation data is completely performed in the HSM in the course of the initial registration process:

1. The identity of the signatory is verified by the certification service provider in accordance with the legal requirements. During the registration process, the signatory has to define the mobile phone number that he/ she wants to use to trigger the signature process in the future and chooses a secret password.
2. The actual possession of the specified mobile phone number is verified by immediately sending an SMS to that device containing an ephemeral one-time-code (transaction number TAN).
3. The signatory has to enter the TAN into a web form.
4. After verification of the TAN by the service, the new signature-creation data is generated in the HSM and this is the same place where this generated private key is immediately encrypted again with another key that is derived from the mobile phone number and the password of the user. Through this, the encrypted private key is only usable later on if the secret password is available for decryption. To also ensure that the usage of the private key is only possible inside the certified HSM, the encrypted private key is encrypted again - this time with a key known only to the HSM. This double-encrypted signature-creation data can be stored even outside of the certified HSM in a key database.

Authentication process

A typical process of authentication may be conducted as follows:

1. A user wants to authenticate against a service provider.
2. The service provider redirects the user to the authentication authority.
3. The user enters his phone number and a password. The password is needed in order to prevent misuse of the service.
4. The authentication authority transmits a TAN valid only for a short time period optionally together with a hash value of the authentication message to be signed to the clients phone via SMS.
5. The user checks the authentication message he is going to sign online, and compares its hash value with the value he has just received.
6. If the values match, the user enters the TAN together with the PIN related to his private key in a web form.
7. The server signs the authentication message using the HSM and the PIN code provided.
8. The result of this signature is sent to the service provider.
9. The service provider performs a signature verification as well as a certificate validation.
10. Upon a successful verification the service provider accepts the user's authentication.

The signing process

The subsequent use of the signature-creation data for signature creation is similar to the described registration process:

1. If a user wants to sign a document, he/ she triggers a signature request of the application in use (be it a web application or locally installed software). This signature

request includes the documents/ data to be signed and is directed towards the provider of the mobile phone signature.

2. As soon as the request is received by the HSM, the user has to enter his/ her mobile phone number (which serves as the User-ID) and his secret password. All these entries are of course processed through secure communication channels directly in the web application of the mobile phone signature.
3. After examining whether the specified number matches a registered signatory, the document/ data to be signed, including the password and phone number, are immediately passed to the HSM. The HSM subsequently calculates a hash value (digital fingerprint) of the document/ data and a random ephemeral one-time code (TAN). Both are sent with an SMS to the specified mobile phone. In parallel, the signatory is offered by the web application of the mobile phone signature service to see and check once again the data to be signed. At the same time, the short hash value is displayed by the web application.
4. The signatory receives the SMS and has the possibility to compare the hash value received by SMS with the hash value displayed by the web application. With entering the received TAN into the web frontend of the mobile phone signature service, it is assured that the signatory is actually in possession of the registered mobile phone.
5. This positive verification causes the HSM, to retrieve the associated encrypted signature-creation data from the key database and to decrypt it with the secret key of the HSM. In the next step, this – still encrypted – signature-creation data is decrypted using the derivation of the secret password of the user. Only now the private key is available in the certified HSM.
6. The signature is created in the HSM and the signed document/ data is handed over to the signatory.

Both, the decryption of the signature-creation data and the creation of the signature itself, are performed exclusively within the certified HSM and the selected decryption mechanisms assure that this is technically possible only there. From this perspective, the security of the created signature is equal to that of a smart-card based solution. Also from the perspective of the signatory, the process is comparable: the signature process is triggered with two components: disclosure of the secret password (factor "knowledge") and mobile phone number and positive verification of the possession of the mobile phone (factor "possession"). The “knowledge” factor is verified by the HSM itself in the process of decryption of the signature-creation data. The verification of the “possession” factor is carried out by the secure signature application, which also includes the connection to the peripheral elements such as SMS gateway or web front end.

Legal requirements for electronic signatures

According to the EU Directive, a qualified electronic signature is an advanced signature based on a qualified certificate and created by a secure-signature-creation device. In the present context, the legal requirements for an advanced electronic signature are[4] :

a) uniquely linked to the signatory;

[4] Art. 2.2 of the Directive

b) capable of identifying the signatory;
c) created using means that the signatory can maintain under his sole control; and
d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Current Moldovan legislation on digital signature, namely Law Nr. 264 from 15.07.2004 about electronic documents and digital signature partly confirms the above mentioned legal requirements. In particular, art. 22 p.2 states that the digital signature means have to ensure that:

a) the digital signature is unique;
b) it makes it very difficult to guess either the private key or the resulting digital signature;
c) the private key is kept confidential

Art. 21 p.5 states that the private key is kept and used exclusively by the signatory, in a way that access of another person to it is excluded.
Currently there is a draft law on digital signature and electronic document which will replace current law nr. 264-XV. The new law is in fact an alignment to European Directive 1999/93 and includes those explicit requirements for digital signature which were described above.

Analysis of mobile identity alternatives

As it was stated, the client side mobile ID is implemented successfully in Estonia, while server side option is successfully implemented by Austria. Fortunately we had the opportunity to discuss with implementation teams of both countries and even had a joint session clarifying different aspects of these two alternatives, such as security, ease of implementation, user uptake, etc.
As a result of consultations with local mobile operators, representatives from national certificate authority and development teams, we came to the following conclusions:

1. Technically both solutions are valid – they solve the problem of mobile authentication and signature.
2. In order to select one alternative for further implementation, the following set of criteria should be applied. These criteria have different relevance to current context in the country which when analyzed could be weighted using a scale from 1 (lowest relevance) to 10 (critical relevance)

#	Criterion	Description
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?
	Implementation timeframe	How long it will take to implement the system? When it could be potentially launched?
	End user uptake: usability	How confortable 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?
	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)?
	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 -
	Technical support	How the users will be supported in using DS? Who will offer that support?
	Private/banking sector uptake	To what extent the private sector will use this national authentication system for their solutions? How many potential companies/banks will be willing to re-use this solution?
	Security	How secure is the storage and transportation of data? What is the user perception of the system's security? What are the chances for loosing sensitive information and what is impact of such loss?
	Reliability of the model	How reliable is the systemas a whole? How many players are involved in the process? What happens if a segment falls, e.g. a user loses his mobile – how fast he/she can start using the system again?
	Non-discrimination	Does this model create a fair competition on the market? Is it an open model anyone could enter?

3. Preliminary analysis of Moldovan regulatory framework related to digital signatures shows that in both cases, some legislative adjustments shall be made in order to implement mobile identity. In the case of client side mobile ID implementation, the operators shall be empowered to map digital identities to natural persons, while in case of server side implementation the legislation shall give clear interpretation that the phrase "signature shall be under signatory sole control" means that the signature must be triggered exclusively by the signatory no matter where the electronic identity is physically kept. This is in fact what new draft law is stating. Due to inevitable adjustments to regulatory framework for both options, this criterion positions both alternatives nearly equally.

Risks

The following major risks are identified:

1. Legal adjustments may take longer than expected.
2. Although scoring may show that server side option is more convenient to be implemented, the private sector (especially some banks) may not accept it due to perception of being less secure.

Next steps

1. To consult private sector, mainly commercial banks (beginning of June-2011), on:
    a. Would they be interested in re-using an authentication service offered by the government?
    b. What option is preferred, particularly keeping in mind time to implement and cost efficiency?
2. To organize a series of meetings with major stakeholders and to evaluate both options using the predefined set of criteria (beginning of June-2011).
3. To identify what are the required changes in the regulatory framework and how the changes should be adopted (mid June-2011).
4. To identify who are the players in the chosen solution and to develop a business model accordingly (mid June-2011).
5. To develop an implementation plan, considering the chosen option and feedback collected during consultations (end of June-2011).
6. To implement the plan (by November-2011).

References

1. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, published in the Official Journal of the European Communities (OJ) L 13, 19.01.2000, See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:EN:PDF
2. Legea Nr. 264 XV din 15/07/2004 cu privire la documentul electronic şi semnătura digitala. http://www.mtic.gov.md/img/pdf/264_2004-07-15_md.pdf

3. Proiectul legii cu privire la semnatura digitala si documentul electronic, 2010.
4. STORK project report, STORK Work Item 3.3.6 Mobile eID
5. Austrian Mobile Phone Signature - an easy-to-use qualified electronic signature as the way to foster trust and security, reliability and authenticity for e-government and beyond, Peter REICHSTÄDTER, Peter KUSTOR, Austira