IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE ICELAND

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Icelandic eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
CA	Certification Authority
CRL	Certificate Revocation Lists
CSP	Certificate Service Provider
eID	Electronic Identity
eIDM	Electronic Identity Management
IAM	Identity and Authentication Management
IDM	Identity Management
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SA	Supervision Authority
SOAP	Simple Object Access Protocol
SCVP	Server-based Certificate Validation Protocol
SSCD	Secure Signature Creation Device
USB	Universal Serial Bus
TTP	Trusted Third Party
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
XML-DSIG	XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

Today there is no central eIDM system for either central or local government in Iceland but the government is in the process of implementing a central eIDM system projected to be ready in Q4 2007.

The Icelandic Governmental agencies use a variety of eIDM systems today, most of which are username/password-based. Some central government agencies have been using soft X.509 certificates in eGovernment since 2003, for example The Internal Tax Revenue Directorate and The Directorate of Customs.

The main policy regarding e-government in Iceland is *"Resources to Serve Everyone - Policy of the Government of Iceland on the Information Society 2004-2007".* In this policy there are some goals that relate to identification. About eID it says *"The policy will be to aim for the general and widespread use of electronic certification so that any communicating partner may be positively identified.."*

The ministry of finance has been running a pilot project for a central eIDM system based on X.509 PKI certificates since 2003. This pilot is planned to be closed next year when a new central eIDM system is expected to be up and running.

Today the government is implementing a central eIDM system in Iceland that is based on X.509 PKI certificates. The main objective of this project is to build an open and standardized X.509 PKI environment in Iceland. From this structure eIDs will be distributed to all citizens in the country. Citizens can use the eIDs in relations to both central and local government as wel as other businesses in Iceland. The Icelandic Government is in co-operation with the Federation of Icelandic Banks in building and implementing this system. The banks will start to distribute certificates on bank cards in Q4 2007 and it is expected that most citizens will have certificates on a smart card before the end of 2008.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

Iceland is a republic, has a written constitution and a parliamentary form of government. The president is elected by direct popular vote for a term of four years, with no term limit. Most executive power rests with the Government, which is elected separately from the presidential elections every four years.

The country is divided into 79 municipalities (local authorities) which are independent but under the supervision of the Ministry of Social Affairs. Their responsibilities lie on social welfare, health, education, cultural matters and infrastructure. The Association of Local Authorities in Iceland is the forum for cooperation between the local authorities.

The policy and strategy on eGovernment is determined by the Prime Minister's Office, which is also responsible for releasing documents such as the plan for 2004-2007 entitled Resources to Serve Everyone, itself a sequel of the previous 1997-2002 plan. The general organisational approach to eGovernment in Iceland is centralised policy and strategy but decentralised implementation.

3.2.2 National eGovernment cooperation and coordination

The policy is coordinated by a steering group called the "Information Society Taskforce", operating under the auspices of the Office of the Prime Minister. This includes assisting public institutions in their efforts towards achieving the main objectives. Related to the policy the Department for the Information Society located at the Prime Minister's Office has a special fund every year to finance IT projects. A special project management team, "The eGovernment Taskforce" focuses on eGovernment issues in the policy. Several other committees are operating as well.

Implementation is undertaken by the Government offices (ministries) according to their role and subject.

The county's policy on eGovernment was put forward in the plan for 2004-2007, published by the Prime Minister's Office under the title: Resources to Serve Everyone. The document is the continuation of the already completed 1997-2003 plan and refers to the overall view for Iceland in the Information Society for 2004-2007.[3]

3.2.3 Traditional identity resources

The main governmental IDs in Iceland are the driver's license, passports (meets ICAO requirements) and national ID cards issued to all citizens when they reach the age of 14 years old. These cards typically include Name, date of birth, Social Security Number (SSN#), validity time, issuance date issuer etc. Bankcards are also generally accepted as IDs because they have a picture and the SSN# on them.

The National Registry under the Ministry of Justice and Ecclesiastical Affairs is responsible for issuing the national ID card, the passport as well as the national register. The National Population Register contains information for all Icelandic persons and for persons with residence permit in Iceland. Persons (both natural persons and legal entities) are identified with a ID-number (SSN#) in the National Register of Persons or in the National Business Register.

[3] http://eng.forsaetisraduneyti.is/media/English/IT_Policy2004.pdf

The ID-numbers are issued at birth to all children born in Iceland and at first registration to all persons that take up domicile in the country. The ID-number system is the only universal one used in the country. The ID-number is a 10-digit number. The register contains information of the personal identification number, name, address, birth registration, citizenship, relations to the national church, kinship, marital status and more.

Anyone can use the SSN# as a unique identifier in their business, but with certain limitations. The main limitation is the general rule about having a just cause to use the SSN#. There is also certain criterion that relates to connecting different data with the SSN# as the key nominator.

Companies and institutions can apply for an ID-number for non-nationals. Non-nationals are registered in a separate registry until they get a residence permit. The Icelandic Directorate of Immigration issues residence permits.

The Internal Revenue Directorate, under the ministry of finance, issues ID numbers to businesses and is responsible for the business registry.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Today there is no central eIDM system for either central or local government in Iceland but the government is in the process of implementing a central eIDM system projected to be ready in Q4 2007. General information on eIDs in Iceland can be found at the eID webpage that is run by the ministry of finance[4], the webpage is currently only in Icelandic.

Today the Icelandic Governmental agencies use a variety of eIDM systems, most of which are username/password-based. Some central government agencies have been using soft X.509 certificates in eGovernment since 2003, for example The Internal Tax Revenue Directorate and The Directorate of Customs.

The main policy regarding e-government in Iceland is *“Resources to Serve Everyone - Policy of the Government of Iceland on the Information Society 2004-2007”.* In this policy there are some goals that relate to identification. It says *“The policy will be to aim for the general and widespread use of electronic certification so that any communicating partner may be positively identified...”*[5]

[4] http://eid.is/

[5] http://eng.forsaetisraduneyti.is/media/English/IT_Policy2004.pdf

The goals related to electronic certification are on the responsibility of the ministry of finance.

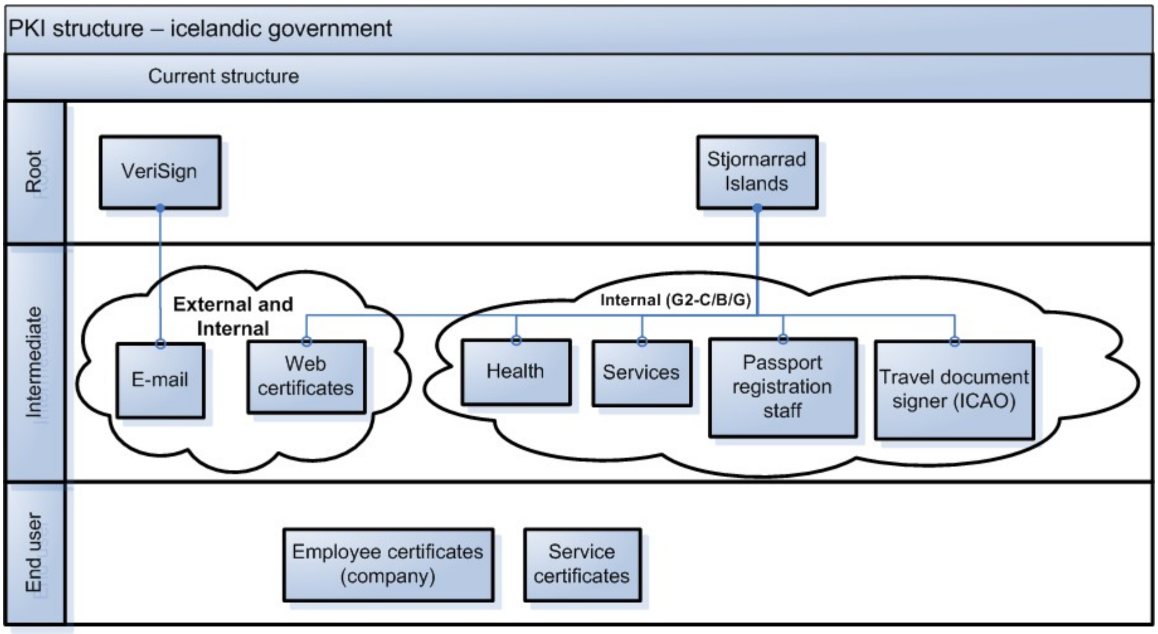
<u>The three goals are:</u>

1. The policy will be to aim for the general and widespread use of electronic certification so that any communicating partner may be positively identified; electronic signatures and coding shall be introduced insofar as is deemed appropriate.

2. An open but standardised market is Iceland's goal, through the use of electronic certificates and certifying services. The state's requirements shall be published with regard to the content, form and handling of electronic certificates for transactions with national institutions. Those requirements might become the model for a general Public Key Infrastructure (PKI) for industry and municipalities. A simple system, economic in operation, should be the object, so that cost may be distributed in proportion to user benefits.

3. European and international standards shall be adhered to, aiming for integration with the Public Key Infrastructure of neighbouring countries when the time seems right.

The ministry of finance has been running a pilot project for a central eIDM system based on X.509 PKI certificates since 2003. The main part of this system is managed by the Directorate of Customs who is responsible for issuing the certificates. Various government agencies have been participating in this project. The current PKI structure is showed on the following picture.



- Current PKI structure for the Icelandic government -

The certificates and supporting systems are licensed from Verisign Corp. through Skýrr hf. There are two main types of certificates:

- a certificate for signing and encrypting e-mail etc.
- a certificate for accessing government web services

This pilot is planned to be closed next year when a new central eIDM system is expected to be up and running.

Today the government is implementing a central eIDM system in Iceland that is based on X.509 PKI certificates. The main objective of this project is to build an open and standardized X.509 PKI environment in Iceland. From this structure eIDs will be distributed to all citizens in the country. Citizens can use the eIDs in relations to both central and local government as well as other businesses in Iceland. The Icelandic Government is in co-operation with the Federation of Icelandic Banks in building and implementing this system.

Citizens will receive X.509 certificates on smartcards, distributed by the Government and also on banking (debit/credit) cards. There will be two certificates on the card, one for authentication and another for signature.

It will be possible to use the certificates for authentication against various online web services in Iceland, including most Governmental web services as well as many web services in the private sector. It will also be used for non-repudiation signatures in any public/private service. Although no certificates have yet been distributed a variety of services already exist and it is expected that there will be a significant number of services by the end of Q4 2007 when rollout of cards and certificates is estimated to begin.

Certificates will be issued to natural persons, employees and software/hardware. The certificates are linked to the entity via the entity's unique identifier (SSN#) which is a part of the certificate content. The certificates contain no specific attributes.

The certificates will be distributed for free and it is estimated that about 80-90% of the population will receive them before Q3 2008.

No immediate decision has been made on whether to offer alternative tokens or certificates in different format (soft certificates), the main focus will be on smart cards.

CRL and OCSP will be freely distributed (at least within reasonable limits).

The above will allow any service provider to set up service for anyone with certificates to use, thus allowing for a market driven system with increased quality of service for all citizens and service providers.

3.3.2 Legal framework

Today there is no legal framework for eIDM system in Iceland. The main legal frameworks that relate to eIDM system are following:[6]

eGovernment legislation

On 10 March 2003 an amendment (No. 51/2003) was approved to the Public Administration Act, No. 37/1993, adding a special chapter on the electronic handling of matters by public administration. Through this modification, general obstacles to the development of electronic administration were removed. While formulating the amendment, the committee in question was guided by the concept of equivalent value, and also emphasised the need to maintain technical impartiality. The alteration involved mere permission for the electronic handling of governmental administration cases, but not an obligation.

Data Protection/Privacy legislation

The Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000, as amended, was passed in 2000 and came into effect on 1 January 2001. The act implements the EC Data Protection Directive and deals with how the protective principle relates to data quality and presented criteria for the legitimacy of data processing. The act applies to any automated processing of personal data and to manual processing of such data if it is, or is intended to become, a part of a file. It has been amended by Act No. 90/2001, Act No. 30/2002, Act No. 81/2002 and Act no. 46/2003.

National registry

The Act on national registry, no. 54/1962 and act on national ID card, no 25/1965.

eSignatures legislation

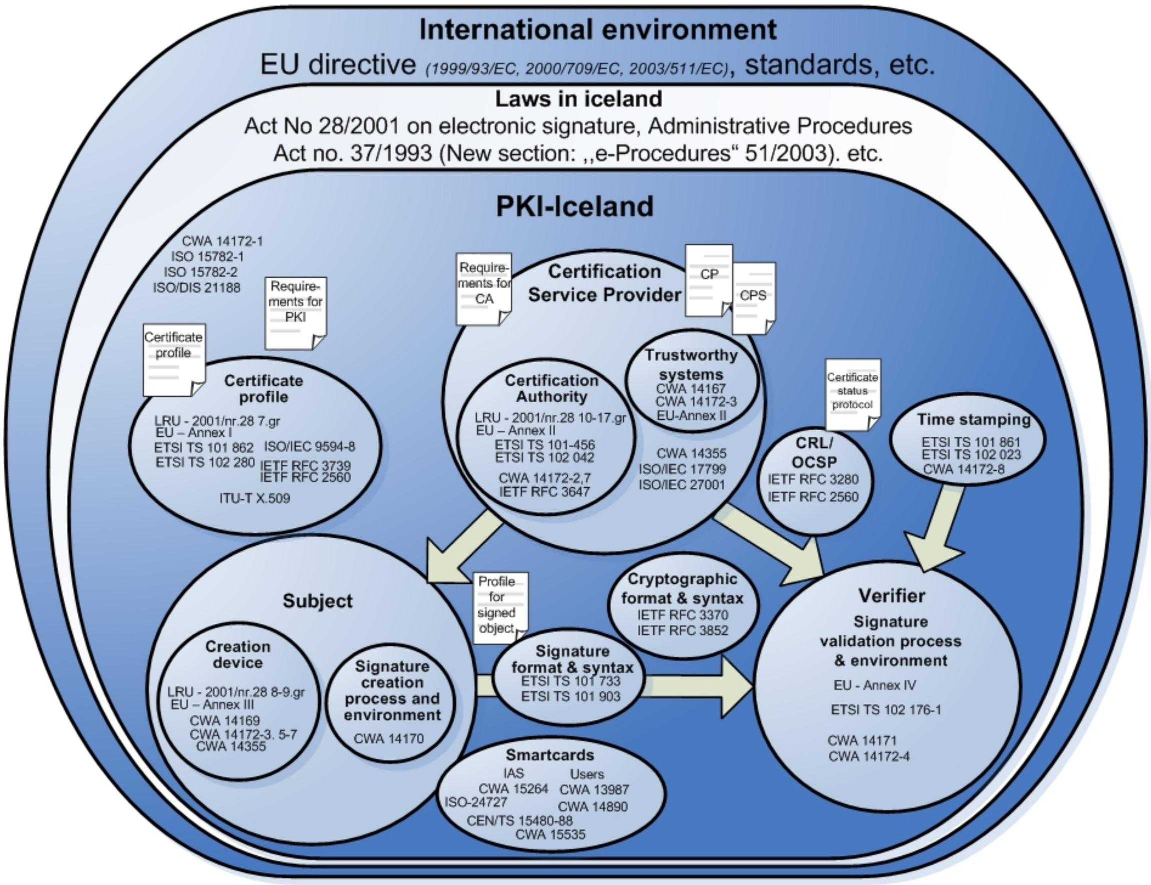
The Government passed a bill on electronic signatures in the spring of 2001, as Act No. 28/2001. Based on the similar EC Directive, article 4 of the Act stipulates that fully qualified electronic signatures shall have the same force as handwritten signatures. Furthermore, it is stipulated that other electronic signatures can be legally binding. Supporting legislation comes through the Electronic Commerce Act, 2002 and the Public Administration Act as amended in 2003.

[6] All laws can be found on the Parliamentary web page, www.althingi.is.

3.3.3 Technical aspects

Today there is no central eIDM system for either central or local government in Iceland. Today the Icelandic governmental agencies use a variety of eIDM systems, most of which are username/password-based. Some central government agencies have been using soft X.509 certificates in eGovernment since 2003, for example The Internal Tax Revenue Directorate and The Directorate of Customs.

The government is currently implementing a central eIDM system in Iceland that is based on X.509 PKI certificates. The main objective of this project is to build an open and standardized X.509 PKI environment in Iceland. The system is projected to be ready in Q4 2007. The environment is described in the following picture.



- PKI environment Iceland -

The environment is structured in three main layers. Firstly there's the international environment, then the main related Icelandic laws, and then the national PKI environment. The PKI-Iceland environment shows three main requirement sets; Certification Service Provider (that includes the Certification Authority), Subject (the one certified) and the verifier (the one that relies on the certificate). In addition, we show the requirement sets for the relations between the entities; certificate profile, the CRL protocols, the format and syntax for signed and encrypted objects, smartcards and the time stamping. In the picture it is attempted to provide an overview of the relevant standards and recommendations in each requirement set. It is realised that there are other standards and recommendations that are references, but the standards and recommendations indicated should be the ones that are directly relevant. It is also indicated what requirement definitions and related documents are needed (shown as pages). Three of them have the scope of the entire PKI (PDS; requirements for PKI and definition of security levels), but others are specific for the requirement sets. The Certification profile[7] can be found at the general webpage about eIDs in Iceland.

Other specific issues:

- ***If any, which of the following authentication mechanisms is used in the eIDM system:***
  - ***a) Public key infrastructure based smart card token***
  - ***b) OTP-Token***
  - ***c) OTP-Password list***
  - ***d) User account/password***
  - ***e) PKCS#12, or other soft tokens***
  - ***f) Other, please specify?***
  - ***g) If several authentication methods are used: is there any difference between services provided to authenticated users?***

    a., d. and e. are being used today.

    Option a. is however likely to become prevalent and completely dominant for any current or future eID service in Iceland

- ***If any, which is the token format chosen in your country IMS?***
  - ***a) Token format is ID1 (e.g. "credit card" format)***
  - ***b) Token format is ID2 (larger (A7) format)***
  - ***c) Token format is ID3 (passport format)***
  - ***d) Other (USB tokens, etc. – please explain)***

    a.

- ***Which is the data storage technology of the ID token?***
  - ***a) Optical encoded data (e.g. 1D or 2D bar codes, OCR-B MRZ, etc.)***
  - ***b) Magnetic stripes (ISO 7811)***
  - ***c) Laser stripes (ISO-11694)***
  - ***d) Contact ICs (ISO 7816, i.e. traditional smart cards). Please specify the EEPROM size available for data***
  - ***e) Contactless ICs (ISO 14443, i.e. RFID). Please specify the EEPROM size available for data.***
  - ***f) Combi-chips (two chips on the same card, one contact and one contactless). Please specify the EEPROM size available for data for both chipsets.***

[7] http://skilriki.is/media/skjol/Innihald_skilrikja_01-04-00.pdf

- ***g) Dual Interface ICs (one chip, two interfaces (contact ISO 7816 and contactless ISO 14443)). Please specify the EEPROM size available for data.***

  Option d. Standardized ISO 7816 cards, support for CEN TC 224 WG 15 / ECC IAS is emphasized. It is estimated that the EEPROM needed for PKI data will be between 8-12k, it is likely that there will be sufficient memory for additional 6-12k.

- ***Does the token have a cryptographic engine or cryptographic capabilities?***
  - ***a) Tokens support only memory chips, without cryptographic functions***
  - ***b) Tokens with cryptographic capabilities are used***
  - ***c) None (no IC on token)***

  Option b. Yes, cards can perform (e.g.) RSA 2048 bit encryption.

- ***If a smart card is used, with respect to the chip memory organization, does the LDS (Logical Data Structure) of the card follow a recognized or proposed standard (e.g. PKCS#15, CEN TC 224 WG 15 ECC Part 2, ICAO LDS 1.7, etc.)?***

  The LDS will follow PKCS#15 and CEN TC 224 WG 15 ECC Part 2 as closely as possible. Both the public and the private sector in Iceland emphasize the adherence to these standards.

- ***With respect to the use of tokens by applications, is the related middleware following a de facto standard, for example PKCS#11, CSP, etc.? Is it independent from the card vendor (i.e. uniquely defined, distributed and maintained by the official card issuer)?***

  The chosen middleware will offer both support for PKCS#11 for Linux and Windows and MS-CSP for Windows a as well as support for Mac OS native CSP.

  The software is supplied by a 3rd party, independent vendor and can be used with chips supplied from different card vendors as long as those chips are compliant with de facto standards.

- ***If the eIDM system is PKI based:***
  - ***Which model of PKI architecture is used? Single CA Model/Hierarchical Model/Mesh Model/Validation authority Model/Web-Internet Trust Model/Bridge Model?***

    Single CA Model/Hierarchical

  - ***If your eIDM system relies on a dedicated PKI infrastructure, then is the CA part of a hierarchy (Sub CA) or it is an independent Root CA?***

    Sub CA

  - ***Is the PKI linked to other PKI infrastructures through an existing Bridge-CA network?***

    No

  - ***Which directory standard is used to publish certificates? (e.g. LDAP).***

    LDAP

- ***Which method for revocation is used? (CRL / Delta-CRL / OCSP)***

  CRL and OCSP

- ***Which are the main back-office components of your country eIDM system?***

  The National Population Register Office which provides everyone with SSN#.

  The National Population Registry (available from the register to almost anyone in Iceland)

  The Iceland Root

  The Iceland eID provider

- ***Does your country subscribe to any of the following standard solution models: Liberty alliance, WS Star, SAML 2.0, or other? If so, are any of those already in use? Please describe any implementation in place.***

  No.

  There is no strategy on this issue today but the government is in the process of mapping these standards with the objective of standardizing the environment in Iceland.

  Currently a few backend Governmental systems make use of SAML for Single-Sign-On procedures.

- ***How can decentralised e-government services (regional/commune/… level) 'plug in' to a national/federal eIDM system, if this has been implemented? Is there a central portal through which services are offered, does the system rely on LDAP protocol, SAML, identity federation,…? In short, how is interoperability within national borders achieved, if at all?***

  As the national eIDM system is by definition a decentralized system there are no restrictions for the usage. Any local Government or private agency can decide to trust the issuer of the certificates. As long as they trust the issuer interoperability is guaranteed. All that is needed is for the local Government to read the certificate content to obtain the unique identifier needed to identify the entity. Validation of certificate is done using standardized methods.

  If there are local trusted third parties how is trust built between the governmental PKI and any trusted third party PKI (cross certification, bridge CA, common CTL list, others)?

  There is no need, at least not yet.

- ***What are the main characteristics of your country's eIDM system with regard to the process of authorisation (if any system has been put in place)?***
  - ***Is a centralized authentication gateway used which recognises different roles, and how?***

    No. Any eIDM token can be used for authentication against any web-service. It is up to the web-service to define the roles or attributes for the entity holding the eIDM-token.

- ***If several different authentication methods are used, are all authorisations treated equally, without distinction based on the authentication method, or can authorisations vary depending on the authentication method..***

  Currently there are different types of authentication methods. With PKI it is likely there will be only one type as PKI (certificates) is the only authentication-method usable for non-repudiation signatures as well.

- ***If role based authorisation is used, then please describe how roles are managed and identified.***

  Not used.

- ***Is any kind of biometry used/planned? If so, which (fingerprints, face, iris, …), and where is it stored? Specify any supported standards, if possible.***

  No

3.3.4 Organisational aspects

As it is today there is no central eIDM system in Iceland. Most organizations use username and a password.

The ministry of finance has been running a pilot project for a central eIDM system based on X.509 PKI certificates since 2003. The main part of this system is managed by the Directorate of Customs who is responsible for issuing the certificates.

The ministry of finance is responsible for building an eIDM system and is currently implementing a system, based on X.509 PKI certificates, projected to be ready Q4 2007. Though the ministry of finance is responsible for building the system and maintaining the general policy it will not be directly issuing any eIDS itself. The main issuers of eIDs to citizens and businesses in Iceland will be banks, on bank cards and the national registry, on citizen cards.

See above for detailed description.

3.4 Interoperability

The key element for participating in a formal eIDM system in Iceland is for the person to have an Icelandic SSN#. If a non-national has an SSN# he should be able to use the same systems as nationals.

Integration of foreign eIDM solutions should be possible. Naturally it is preferred that any solution to be accepted by the Icelandic Government follow de facto / industry standards and is based on strong authentication.

The main policy regarding e-government in Iceland is *"Resources to Serve Everyone - Policy of the Government of Iceland on the Information Society 2004-2007".* In this policy there are some goals that relate to interoperability. It states the following:

"European and international standards shall be adhered to, aiming for integration with the Public Key Infrastructure of neighbouring countries when the time seems right."[8]

3.5 eIDM Applications

Today most applications use username and password for electronic authentication. A few use and support digital certificates. Following is an example of applications where people can log into the system in the internet.

Services for citizens

- Income Tax Declaration

  Citizens have been allowed to submit electronic tax returns since 1999 and in 2006 92% filed their taxes electronically. Citizens can use either a certificate or username and a password for accessing the tax portal.
- University of Iceland. Students can log into their "mypage" with either a certificate or username and a password.
- Local Governmental service portals (my pages). Some portals accept certificates, most use username and password.

Services for businesses

- Corporation Tax: declaration, notification

  Business have been allowed to submit electronic tax returns since 1997 and In 2006 95% filed their taxes electronically. Accountants that submit electronic tax returns for their customers use X.509 certificates for authentication and to sign the tax returns.
- VAT: declaration, notification (only username and password.)
- Customs declaration

  The 1996 amendment to the Customs Act, imposed electronic submissions of all custom reports fore import and export companies since 2001. Companies submitting on the Internet need to use using digital certificates for authentication.

When the new eIDM system will be in place and majority of citizens will have certificates on smartcards it is expected that most governmental applications, that have a need for authentication of citizens and businesses, will use this infrastructure. Many governmental agencies are already ready for this or are preparing their systems. This infrastructure will also be open for the private sector and it is expected that many applications will use it by the end of next year. Banks will e.g. use this for their customers for online banking.

[8] http://eng.forsaetisraduneyti.is/media/English/IT_Policy2004.pdf, page 19 nr. 3.

It will be possible to use the certificates for authentication against various online web services in Iceland, including most governmental web services as well as many web services in the private sector.

It is expected that the number of services will be close to 100 by the end of Q4 2007 and 200 by the end of 2008.

3.6 Future trends/expectations

The current eIDM infrastructure does not meet users' needs. The government is currently building an eIDM infrastructure that relies on X.509 PKI infrastructure. The main objective is to use this infrastructure to support a general and widespread use of electronic certification so that any communicating partner may be positively identified.

EIDs will be distributed on bank cards before the end of 2007. The National registry is also expected to issue eIDs that will then be distributed on a citizen card. There are no plans to make eID cards mandatory for citizens but in the future it might be the only way for communication with various eGovernment services.

In the future the infrastructure that is currently being implemented will be used to distribute X.509 PKI certificates with other means like on mobile phones or other secure devices.

Icelandic government is open for interoperability between countries for eCommerce (procurement), e-Authentication for web services and e-Identification at borders and believes that an X.509 PKI environment will be the standard for communication in the future.

3.7 Assessment

The current eIDM infrastructure does not meet users' needs. The government is currently building an eIDM infrastructure that relies on X.509 PKI infrastructure. The main objective is to use this infrastructure to support a general and widespread use of electronic certification so that any communicating partner may be positively identified.

The fact that even without any certificates in the field, there is a number of different services available that support PKI certificates gives an indication that a key factor in the project is to use an open standardized approach to allow for easy uptake by service providers, thus enabling them to offer any kind of service to individuals and companies.

Lack of a central eIDM system for government agencies in Iceland has been seen, by many, as a major hinder in further development in eGovernment in Iceland. The eIDM system that is currently being implemented is expected to have a big impact on eGovernment, both for central and local government.

General and widespread distribution and use of electronic certification on smartcards to citizens and business is seen as a key element in simplifying communication with government and reducing administrative burden.