IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE LATVIA

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 Latvian 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

The most significant and advanced eIDM system in Latvia is based on the smart card holding a certificate for qualified signatures used for creation of electronic signatures and an unqualified authentication certificate used for authentication and stamping of electronic documents with time-stamps. This eIDM system is intended to facilitate access to eGovernment services, as well as offering access to a variety of other services. The first trusted certification service provider VAS Latvijas Pasts started providing qualified certificates for natural and legal persons in October 2006.

No alternative tokens have been introduced in Latvia yet. An introduction of eID cards is planned for the second half of the year 2008, which would contain qualified certificates.

Within the framework of this profile we also describe the only eGovernment application using electronic signatures and the sole eGovernment application relying on basic electronic identification.

All the above-mentioned systems will be discussed in greater detail below.

Currently no public statistics regarding potential user base, actual penetration and actual use of smart cards, i.e. secure means of creation of electronic signatures are available. Likewise there are no statistics on the actual use of the other applications; however, the number of users of these applications is increasing.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

Latvia is a unitary state, and eGovernment consists of state and municipal applications. For development of eGovernment services usually the Secretariat of Special Assignments Minister for Electronic Government Affairs is responsible, however there are some exceptions regarding specific applications, e.g. the Commercial Register is responsible for the introduction of an opportunity to register merchants electronically, the Food and Veterinary Service is responsible for the introduction of an opportunity to electronically register merchants engaged in food circulation, etc. Local eGovernment initiatives are led and coordinated by local authorities, mostly municipalities.

Currently eGovernment services in Latvia mainly consist of provision of information to the public on web sites of state and municipal institutions, downloading of document forms (that have to be submitted in paper format after them filling in) and simple authentication for logging into the systems.

However, eGovernment is developing rapidly. Besides the introduction of a qualified electronic signature in October 2006 other activities are being carried out for making state administration more effective, accessible to the general public and capable of processing qualified electronic signatures, e.g. electronisation of the fields of state administration, in which currently electronic services are not available at all.

Until the introduction of a qualified electronic signature in October 2006 only electronic signatures were used in eGovernment applications. The sole provider of services using electronic signatures was and continues to be the State Revenue Service. Details of this application are assessed in below sections of this report.

Since October 2006 all state and municipal institutions are obliged to accept electronic documents signed with the qualified electronic signature. Readiness to accept such documents varies from institution to institution, however currently it is impossible to precisely assess the real situation with this respect in the state and municipal sector. The tendency is, however, that the number of state and municipal institutions ensuring acceptance of electronic documents signed with a qualified electronic signature is increasing constantly.

3.2.2 Traditional identity resources

Identification towards Latvian eGovernment services traditionally relied mostly on the Population Register. According to the Population Register Law (Article 10) in the population register should be stored following information about natural persons:

1. Identification code;
2. Name or names;
3. Surname;
4. Maiden name or person's initial surname;
5. Date and place of birth;
6. Gender;
7. Citizenship;
8. Nationality;
9. Registered addresses in Latvia;
10. Address in the foreign countries;
11. Information about passport or other identification document;
12. Information about registration of the birth;
13. Information about birth certificate;
14. Information about residence permit in Latvia;
15. Date when person arrived to Latvia if the person is not citizen

of Latvia;
16. Information about marital status, namely not married, divorced, married, widow or widower;
17. Information about last spouse;
18. Information about registration of marriage or divorce;
19. Information about document that testify marriage or divorce;
20. Information about person's children that are younger that 16 years;
21. Information about person's parents;
22. Information about migration, including information about deportation from Latvia;
23. Information about death of the person and registration of the death

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Identifiers, registers and tokens in present solutions - eIDM system based on the smart card, EDS and eProcurement

The most relevant eIDM system is based on the smart card containing a certificate for qualified signatures used for creation of electronic signature and unqualified authentication certificate used for authentication and stamping of electronic documents with time-stamps.

The sole eGovernment application using electronic signatures is the Electronic Declaration System ("EDS") set up by the State Revenue Service. EDS is operational since 2001. However, until March 2006 all documents submitted to the State Revenue Service via EDS needed to be submitted in paper as well. In March 2006 the State Revenue Service adopted an instruction No. 1 "Agreement on signing electronic documents with the electronic signature using the State Revenue Service electronic declaration system services, and ensuring these services", according to which the State Revenue Service and its clients (any natural or legal person) may conclude an agreement on the use of EDS (the "Agreement") and after a conclusion of the Agreement documents submitted to the State Revenue Service via EDS need not be submitted in a paper format any more. Approximately 95% of all the reports and declarations prescribed under Latvian law can be submitted to the State Revenue Service by means of the EDS.

The credentials are issued and managed by the State Revenue Service. Within 5 days from the conclusion of the Agreement the system administrator registers the user and sends to his e-mail address necessary identification data and the initial password. The signature is created using the private key data automatically saved on the electronic signature creation directory in the computer of the user. The user is requested to indicate the location of the private key data file. After receiving the encoded data, the State Revenue Service verifies the signature by comparing the difference of the "hash function" calculated using the State Revenue Service key and the private key of the client.

EDS ensures that the application forms can either be submitted via the web page of the State Revenue Service or by sending to the State Revenue Service previously prepared files with declaration data, i.e. exporting the data by means of files in a specific format from accounting programs of clients and importing them into data bases of the State Revenue Service.

The system relies on an EDS server certificate (data is sent using SSL (Secure Sockets Layer) data protocol). The tax payer signs the entire declaration in question. When the user has filled in his declaration, he is prompted to click on the button "sign and submit" which appears only if the person has the signatory rights.

Currently the electronic signature provided by the State Revenue Service is different from the qualified electronic signature as provided according to the Electronic Documents Law. Nevertheless, the State Revenue Service is ready to accept electronic documents signed by the qualified electronic signature.

There are no specific policies of the state with respect to the eGovernment application in question, and no government initiatives have been introduced with regard to this type of electronic signature. Everything is defined by the Agreement.

The only eGovernment application relying on basic electronic identification is eProcurement. For each service provider and contracting entity a paper token is given, on which access codes are typed. When entering the system, the user is required to enter one of the requested access codes. No specific electronic signature is necessary for using the system. Verification data is stored on the server of the eProcurement system. Access codes entered by the users are verified with those stored on the server. No specific term for validity of entry codes are set.

Currently there are no universal or sector based identifiers, all the identifiers are application specific.

The eIDM system based on the smart card and EDS rely on information from the official registers – mainly the Population Register, and for EDS also from the Commercial Register - in order to identify users of the systems. Information contained in the official registers is not kept on the tokens of the afore-mentioned systems and the eProcurement system.

The planned eID card

The system of eID cards will be based on information contained in the Population Register of the Republic of Latvia. The legislative framework for the introduction of the eID cards is in place, it is the infrastructure that is in the preparation process. According to information provided to us by the Office of Citizenship and Migration Affairs, which is the state institution carrying out the implementation of the system of eID cards, a Development programme of the system of eID cards will be submitted to the Cabinet of Ministers within May 2007. Implementation of the system will most likely start in the second half of the year 2008. There will be the following types of eID cards: a citizen's identity card, a non-citizen's identity card, an identity card for a person who has been granted alternative status, an identity card for a non-resident, i.e. a staff member of a diplomatic or consular representation of a foreign state or an international organisation accredited in Latvia and an identity card for a person who has been granted temporary protection. It will be mandatory for the above-mentioned persons that have reached the age of 15.

Chip of the eID card will be used as a means of creation of a person's electronic signature.

Authentication policies

There is no official authentication policy in Latvia that defines a strict hierarchy of the different authentication systems in use. Currently two types of authentication systems are used – non-PKI electronic signature authentication, and login information (usernames, passwords).

Regional/local applications

Regional/local applications are entirely distinct.

3.3.2 Legal framework

National regulation title	National regulation translated title (English title)	Relevant links to on-line resources
Elektronisko dokumentu likums (sp•k• no 2003. gada 1. janv•ra)	Electronic Documents Law (effective as of 1 January 2003)	http://www.eps.gov.lv/files/juridiskabaze/likumi/EDL.doc
Publisko iepirkumu likums (sp•k• no 2006.gada 1. maija)	Public Procurement Law (effective as of 1 May 2006)	http://www.iub.gov.lv/iub/images/modules/items/item_file_1542_pil.doc
Par iepirkumu sabiedrisko pakalpojumu sniedz•ju vajadz•b•m (sp•k• no 2004. gada 10.	Law On Procurement for the Needs of Public Service Providers (effective as of 10 November 2004)	http://www.iub.gov.lv/iub/images/modules/items/item_file_1552_sps_likums.doc

novembra)		
Ministru Kabineta noteikumi Nr. 473 Elektronisko dokumentu izstr•d•šanas, noform•šanas, glab•šanas un aprites k•rt•ba valsts un pašvald•bu iest•d•s un k•rt•ba, k•d• notiek elektronisko dokumentu aprite starp valsts un pašvald•bu iest•d•m vai starp š•m iest•d•m un fiziskaj•m un juridiskaj•m person•m (pie•emti 2005. gada 28. j•nij•)	Regulations of the Cabinet of Ministers No. 473 on order of elaboration, formatting, storage and circulation of electronic documents in state and municipal institutions and order of circulation of electronic documents among state and municipal institutions and natural and legal persons (adopted on 28 June 2005)	http://www.eps.gov.lv/files/juridiskabaze/edoc_ekspluat_kart_valsts%20iest_Nr.473_28.06.2005.doc
Vienošan•s par elektronisko dokumentu parakst•šanu ar elektronisko parakstu, izmantojot Valsts ie••mumu dienesta elektronisk•s deklar•šanas sist•mas pakalpojumus, un šo pakalpojumu nodrošin•šana (sp•k• no 2006. gada 24. marta)	The State Revenue Service instruction No. 1 Agreement on signing electronic documents with the electronic signature using the State Revenue Service electronic declaration system services, and ensuring these services (effective as of 24 March 2006)	http://www.vid.gov.lv/dokumenti/noderigi/eds/instrukcija nr.1.pdf
Latvijas e-p•rvaldes koncepcija (pie•emta 2002. gada 20. august•)	Latvian eGovernment conception (adopted on 20 August 2002)	http://www.eps.gov.lv/files/projekti/E-parvaldes_koncepcija.pdf
Elektronisk•s p•rvaldes att•st•bas programma 2005. -	eGovernment Development Program for years 2005 – 2009 (approved by order No. 623 of the	http://www.eps.gov.lv/files/projekti/eparv_progr.doc

2009. gadam (apstiprin•ta ar Ministru kabineta 2005.gada 29.septembra r•kojumu Nr. 623)	Cabinet of Ministers as of 29 September 2005)	
Personu apliecinošu dokumentu likums (sp•k• no 2002. gada 1. j•lija)	Personal Identification Documents Law (effective as of 1 July 2002)	http://www.pmlp.gov.lv/images/documents/personaapliecibas.doc
Ministru Kabineta noteikumi Nr. 378 par pilso•u personas apliec•b•m, nepilso•u personas apliec•b•m, pilso•u pas•m, nepilso•u pas•m un bezvalstnieku ce•ošanas dokumentiem (pie•emti 2004. gada 22. apr•l•)	Regulations of the Cabinet of Ministers No. 378 regarding identity cards of citizens and non-citizens, passports of citizens and non-citizens, and travelling documents for stateless persons (adopted on 22 April 2004)	http://www.pmlp.gov.lv/images/documents/pases.doc
Iedz•vot•ju re•istra likums (sp•k• no 1998. gada 24. septembra)	Population Register Law (effective as of 24 September 1998)	http://www.pmlp.gov.lv/images/documents/reg.doc
Fizisko personu datu aizsardz•bas likums (sp•k• no 2000. gada 20. apr••a)	Personal Data Protection Law (effective as of 20 April 2000)	http://www.dvi.gov.lv/likumdosana/fpda/

It should be noted though that Latvia has no specific regulations with regard to the process of authentication in general. Electronic Documents Law effective as of 1 January 2003 transposes the provisions of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, but does not apply to authentication as such.

The main data contained in the Population Register and used by the eIDM systems is the unique personal identity number of a person. According to the Population Register Law, the access to the information contained in the Population Register is very restricted for the private sector entities. Usually a private individual can obtain information about himself, but the entities that require any information from it for carrying out their commercial activity have to write a motivated application to the Office of Citizenship and Migration Affairs and may conclude an agreement with it for specific information required, and the information flow is being controlled by the state.

According to the recent amendments to the Personal Data Protection Law that will become effective as of 1 September 2007, use of personal identity numbers will also be more restricted. Entities requiring individuals to indicate their personal identity numbers will need to indicate the purposes of such usage more specifically.

eIDM systems can be used by the private sector as the clients of the eIDM systems.

eIDM system based on the smart card may be used by individuals and legal entities. In case of use by legal entities, during the application for the tokens, a representative of the legal entity indicates the persons who will represent it, and the tokens are issued to the respective individuals.

As regards EDS, it also may be used by natural and legal persons. Legal entities submit a list of the natural persons entitled to sign on its behalf and their powers to the State Revenue Service, which ensures these persons with the relevant credentials. If more than one person is authorised for the use of the electronic signature, a manager of the electronic signature can be appointed. The manager confers the signatory powers to the users. If the manager has not conferred the signatory powers, the user will not be able to use the electronic signature since no option "sign and submit" will be provided for such person in EDS. The electronic documents cannot be signed by more than one person at a time.

3.3.3 Technical aspects

eIDM system based on the smart card

1. If any, which of the following authentication mechanisms is used in the eIDM system: o a) Public key infrastructure based smart card token o b) OTP-Token o c) OTP-Password list o d) User account/password o e) PKCS#12, or other soft tokens o f) Other, please specify? o g) If several authentication methods are used: is there any difference between services provided to authenticated users?	(a) currently, (e) planned. When (e) will be introduced, there will be a differentiation between services available for holders of different certificate tokens.

- If any, which is the token format chosen in your country IMS? o a) Token format is ID1 (e.g. “credit card” format) o b) Token format is ID2 (larger (A7) format) o c) Token format is ID3 (passport format) o d) Other (USB tokens, etc. – please explain)	Currently only (a), (d) could be introduced in 2-3 years (USB token with advanced holder authentication by fingerprints)
- Which is the data storage technology of the ID token? o a) Optical encoded data (e.g. 1D or 2D bar codes, OCR-B MRZ, etc.) o b) Magnetic stripes (ISO 7811) o c) Laser stripes (ISO-11694) o d) Contact ICs (ISO 7816, i.e. traditional smart cards). Please specify the EEPROM size available for data o e) Contactless ICs (ISO 14443, i.e. RFID). Please specify the EEPROM size available for data. o 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. o g) Dual Interface ICs (one chip, two interfaces (contact ISO 7816 and contact-less ISO 14443)). Please specify the EEPROM size available for data.	(d), 64KB
- Does the token have a cryptographic engine or cryptographic capabilities? o a) Tokens support only memory chips, without cryptographic functions o b) Tokens with cryptographic capabilities are used o c) None (no IC on token)	(b)
- 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.)?	PKCS#15
- 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)?	PKCS#11

- If the eIDM system is PKI based: o Which model of PKI architecture is used? Single CA Model/Hierarchical Model/Mesh Model/Validation authority Model/Web-Internet Trust Model/Bridge Model? o 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? o Is the PKI linked to other PKI infrastructures through an existing Bridge-CA network? o Which directory standard is used to publish certificates? (e.g. LDAP) o Which method for revocation is used? (CRL / Delta-CRL / OCSP)	Hierarchial CA Model Independent Root Currently PKI infrastructure is not linked to any other, but this is planned for 2007. LDAP v3.0 All methods are used: CRL & Delta CRL, & OCSP.
- Which are the main back-office components of your country eIDM system?	Microsoft CA, Custom Registration Processing system, Custom Certificates database, Publication and External interface systems.
Most often the back office is constituted by components such as a Trust Provider (PKI, Doc Signer, etc.), a central or decentralised repository of identity attributes (e.g. a civil register), a biometric database such as an Automatic Fingerprint Identification System (AFIS), or an Identity Provider (IP).	
- 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.
- 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?	The existing solution is the only trusted eIDM solution in operation.
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)?	The existing solution is the only trusted eIDM solution in operation.

- 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)? o Is a centralized authentication gateway used which recognises different roles, and how? o 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.. o If role based authorisation is used, then please describe how roles are managed and identified.	There is a custom rights management module, based on MS Active Directory. All users are authenticated based on smart card tokens issued by the system itself. Roles ar described and managed according to internal documentation, which is supervised by the Certification Services Manager and the Security Offcer. Changes in roles are approved according to standard processes.
- Is any kind of biometry used/planned? If so, which (fingerprints, face, iris, …), and where is it stored? Specify any supported standards, if possible.	Biometry is not used. In future the introduction of USB tokens with fingerprint scanners is planned, however no details of this project are available at this point.

EDS

2. If any, which of the following authentication mechanisms is used in the eIDM system: o a) Public key infrastructure based smart card token o b) OTP-Token o c) OTP-Password list o d) User account/password o e) PKCS#12, or other soft tokens o f) Other, please specify? o g) If several authentication methods are used: is there any difference between services provided to authenticated users?	There is an idea to bond the present electronic signature with the qualified electronic signature. Currently the State Revenue Service accepts the documents signed by the qualified electronic signature, i.e. there is an opportunity to submit the necessary documents to the State Revenue Service without using EDS.

- If any, which is the token format chosen in your country IMS? o a) Token format is ID1 (e.g. “credit card” format) o b) Token format is ID2 (larger (A7) format) o c) Token format is ID3 (passport format) o d) Other (USB tokens, etc. – please explain)	
- Which is the data storage technology of the ID token? o a) Optical encoded data (e.g. 1D or 2D bar codes, OCR-B MRZ, etc.) o b) Magnetic stripes (ISO 7811) o c) Laser stripes (ISO-11694) o d) Contact ICs (ISO 7816, i.e. traditional smart cards). Please specify the EEPROM size available for data o e) Contactless ICs (ISO 14443, i.e. RFID). Please specify the EEPROM size available for data. o 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. o g) Dual Interface ICs (one chip, two interfaces (contact ISO 7816 and contact-less ISO 14443)). Please specify the EEPROM size available for data.	
- Does the token have a cryptographic engine or cryptographic capabilities? o a) Tokens support only memory chips, without cryptographic functions o b) Tokens with cryptographic capabilities are used o c) None (no IC on token)	1024 bits Certificate has been issued by verisign.com.
- 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.)?	
- 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)?	

- If the eIDM system is PKI based: o Which model of PKI architecture is used? Single CA Model/Hierarchical Model/Mesh Model/Validation authority Model/Web-Internet Trust Model/Bridge Model? o 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? o Is the PKI linked to other PKI infrastructures through an existing Bridge-CA network? o Which directory standard is used to publish certificates? (e.g. LDAP) o Which method for revocation is used? (CRL / Delta-CRL / OCSP)	
- Which are the main back-office components of your country eIDM system?	
Most often the back office is constituted by components such as a Trust Provider (PKI, Doc Signer, etc.), a central or decentralised repository of identity attributes (e.g. a civil register), a biometric database such as an Automatic Fingerprint Identification System (AFIS), or an Identity Provider (IP).	
- 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.	
- 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?	The system has been established and is used solely for the needs of the State Revenue Service.
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)?	

- 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)? o Is a centralized authentication gateway used which recognises different roles, and how? o 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.. o If role based authorisation is used, then please describe how roles are managed and identified.	The system is wholly administered by the State Revenue Service.
- Is any kind of biometry used/planned? If so, which (fingerprints, face, iris, …), and where is it stored? Specify any supported standards, if possible.	

3.3.4 Organisational aspects

eIDM system based on the smart card

- How does one get entered into an eIDM system? Who manages the system, i.e. who enters and maintains the information? Is it decentralised/centralised, and who can access the information?	Information is collected by the Registration Operator. Upon verification of the data with the Population Register it is approved by the Registration Officer. Data input is decentralized, approval and storage are centralized. Data access is roles-based.
- Are federated identities in use? If so how is federation built? Is there identity management software in use? Is there a sector based approach? How?	No.
- If role management is used, describe how roles are identified?	There are administrative, operational, technical and security roles. Identification is based on a role model, which is a part of organisational and security documentation of Certification Services organization.
- Who issues eIDM tokens? To whom?	Tokens are issued by Issuing Operators to persons, whose completed applications have been approved by the Registration Officer and processed by the system, upon positive visual identification by means of a valid ID document,

	i.e. passport.
- Who verifies the information included in the eIDM system, and who is responsible for errors?	Registration Operator is responsible for input data, and the Registration Officer is responsible for verified data.
- Can the user verify what information of his is accessed or passed onto third parties, and by whom? How?	Upon written application the Certification Service provider will deliver a report on manipulations performed on data of a natural person. Upon applying for services the natural person is asked to issue a written consent regarding the use of his/her data for certification services needs.

EDS

- How does one get entered into an eIDM system? Who manages the system, i.e. who enters and maintains the information? Is it decentralised/centralised, and who can access the information?	The system is wholly administered by the State Revenue Service. Details are considered as sensitive data.
- Are federated identities in use? If so how is federation built? Is there identity management software in use? Is there a sector based approach? How?	
- If role management is used, describe how roles are identified?	
- Who issues eIDM tokens? To whom?	State Revenue Service issues the tokens to the users of the system.
- Who verifies the information included in the eIDM system, and who is responsible for errors?	State Revenue Service
- Can the user verify what information of his is accessed or passed onto third parties, and by whom? How?	No information is currently accessed by or passed to third parties. In future the State Revenue Service might cooperate with the Commercial Register, as the annual reports have to be submitted to both of the above-mentioned institutions. However, no such solutions have been developed yet.

3.4 Interoperability

The eIDM system based on the smart card is available only to persons holding a passport issued in the Republic of Latvia.

The EDS system is accessible to non-nationals if they have concluded the Agreement[3]. The State Revenue Service has not taken any measures to ensure interoperability with signatures created and/or certificates issued in other countries.

The eProcurement system is accessible to any contracting entity and supplier of goods that have concluded an agreement with the Electronic Procurement State Agency.

3.5 eIDM Applications

According to Electronic Documents Law and Regulations of the Cabinet of Ministers No. 473 as of 28 June 2005 on order of elaboration, formatting, storage and circulation of electronic documents in state and municipal institutions and order of circulation of electronic documents among state and municipal institutions and natural and legal persons all state and municipal authorities, as well as private entities have to accept documents signed by a qualified electronic signature issued by VAS Latvijas Pasts.

However, practical use of the qualified electronic signature has been very insignificant due to a lack of information regarding it for the general public and the insignificant number of eGovernment services available by using it.

Currently the following state authorities have explicitly indicated their ability to accept the documents signed by a qualified electronic signature:

a) Office of Citizenship and Migration Affairs (since 1 January 2007 mandatory declaration of the place of residence can be carried out by sending an application signed by a qualified electronic signature to the e-mail address deklaracija@pmlp.gov.lv);

b) State Social Security Agency (since February 2007 documents signed by a qualified electronic signature can be sent to the e-mail address edoc@vsaa.lv);

c) Road Traffic Security Office (since April 2007 documents signed by a qualified electronic signature can be sent to the e-mail address eoffice@csdd.gov.lv; in addition, a qualified electronic signature can be used in order to access data about oneself contained in the State Register of the Vehicles and Drivers with respect to owned vehicles and the driver, i.e. the driver's licence, fines, etc.);

[3] Please see Section D.1.1 above.

d) State Revenue Service (accepts documents signed by a qualified electronic signature with any respect).

In the private sector the biggest bank in Latvia AS Hansabanka has explicitly stated that the smart card can be used for authentication in its internet banking system. The qualified electronic signature can be used instead of the code card or code calculator issued by the bank for authentication purposes.

No other public information is available on usage of the qualified electronic signature in the private sector.

3.6 Future trends/expectations

The most relevant development will be the introduction of the mandatory eID card in the second half of the year 2008. However, no detailed description of the solution is available at this point.

Currently state and municipal authorities are trying to ensure access to their services by means of the qualified electronic signature, which will be a time-consuming process.

The eProcurement system is planned to be used as a basis for carrying out eAuctioneering within general procedures that are not electronically handled. Legal framework has already been established, however at the moment contracting entities do not have proper IT solutions to handle eAuctioneering.

3.7 Assessment

In our opinion the Latvian eIDM infrastructure is still underdeveloped in comparison with other EU member states. Introduction of eID cards has been postponed several times for several years, and the same applied to the qualified electronic signature before its introduction in 2006.

Moreover, already at the time of introduction of the qualified electronic signature it was clear that the ability to ensure circulation of the documents signed by a qualified electronic signature by the state and municipal authorities would be very limited. It is constantly developing, however currently availability of a very narrow scope of public services by using the qualified electronic signature is ensured. Therefore, we consider that currently the motivation for using the qualified electronic signature is objectively low.

As regards EDS, it is a system that plays a relevant role in the Latvian eGovernment infrastructure. Services of the State Revenue Service are mandatory for a considerable part of the population. Therefore, EDS substantially increases efficiency of cooperation between the State Revenue Service and natural and legal persons.

The Latvian eIDM system based on smart cards is largely built for Latvian nationals. EDS and eProcurement systems are however available to anybody having concluded respective agreements, as described above.