eID Interoperability for PEGS

NATIONAL PROFILE LITHUANIA

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

© European Communities, 2007

Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.

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 Lithuanian 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

None of the eIDM systems operating in Lithuania constitute a uniform user authentication mechanism for all eGovernment services. However, the majority of the eIDM systems of the public sector in Lithuania rely on authentication systems of the private sector, namely eBanking authentication means.

The portal Government Electronic Gates[3] (the "Portal") is the front-office application intended for access to eGovernment services from one place. At present, however, the number of eGovernment services available in the portal is limited.

eBanking authentication means are used upon agreement with commercial banks and form the basis for user authentication both in Government Electronic Gates portal and in other separate eGovernment applications, providing interactive services independently from the Portal.

Other eIDM systems are based on personal certificates of 2nd and 3rd class, issued by qualified certification services providers, or usernames and passwords.

As regards future plans concerning eIDM systems, the introduction of an eID card is anticipated. In the current stage a feasibility study is prepared and application for financing is to be made. The appearance of the eID and other details are not therefore certain yet. Other initiatives include SIM cards of mobile phones containing PKI certificates.

Authentication information of natural persons is stored in the Residents' Register. The main identifier is the personal code. As regards legal persons, their data is kept within the Register of Legal Persons, the key identifier being legal person's code.

[3] See https://paslaugos.evaldzia.lt.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

In Lithuania eGovernment projects are vertically integrated, i.e. operating within one sector such as tax reporting, submission of statistical reports, financial statements reporting etc. Different technological solutions have been chosen for each of the applications with separate legal acts on provision of each of the electronic services. Nevertheless, steps are being taken towards horizontal integration covering several departments and institutions.

The framework document for eGovernment services which has harmonizing effect is the Position Paper on eGovernment[4]. The Position Paper stipulates the introduction of eGovernment in order to render the governance of the state more open, democratic, accountable and effective. It states among other things, that when anticipating new public services no obstacles should be created for electronic transactions, e.g. there should be no requirement of handwritten signature. The Position Paper also states that eGovernment projects shall operate regardless of the eSignature infrastructure in Lithuania, therefore other means may be applied where authentication of the user and safe connection between the user and the server are ensured. This provision opened the gate for a series of eGovernment applications, based on entity authentication.

The Position Paper provides for 4 stages for transposition online of eGovernment services: from mere placement of relevant information online (1st level) to completely interactive eGovernment service (4th level).

The Plan on Implementation Measures of the Position Paper on eGovernment[5] lays down the targets to be reached in various eGovernment services by the end of the year 2012, specifying the anticipated level of transmission online of each eGovernment service.

There are three principal state institutions responsible for the eGovernment domain: the Ministry of the Interior (Department of eGovernment services)[6], the Information Society Development Committee under the Government of the Republic of Lithuania[7] (the "Committee") and the Information Society Development Committee of the Parliament.[8]

[4] Adopted by Decree No 2115 of the Government of the Republic of Lithuania as of 31 December 2002; 2002 m. gruodžio 31 d. Vyriausyb• s nutarimas d• l elektronin• s valdžios koncepcijos patvirtinimo Nr. 2115.

[5] Adopted by the Decree No 1468 of the Government of the Republic of Lithuania as of 25 November 2003.

[6] Vidaus reikal• ministerija (E. valdžios paslaug• skyrius).

[7] Informacin• s visuomen• s pl• tros komitetas prie Vidaus reikal• ministerijos.

[8] Seimo informacin• s visuomen• s pl• tros komitetas.

The Ministry of the Interior[9] is vested with powers of management of eGovernment projects and supervision of rendering of public services with the help of digital technologies.

The Committee[10] is the state institution responsible for coordination and supervision of eGovernment projects. Among other functions the Committee participates in implementation of the state's policy of using eSignature. The Department of registers and IT systems of the Committee[11] coordinates projecting, implementation, interoperability and use of integral system of the state's registers and data basis of common use.

The Information Society Development Committee of the Parliament drafts legal acts, proposes policy on the development of the information society, submits proposals and opinions to the Parliament in the domain of information society.

Horizontal integration of eGovernment services is driven by the eGovernment portal (www.evaldzia.lt, www.epaslaugos.lt, www.govonline.lt) administered by the Committee[12]. The website, however, only provides the list of state and municipal institutions and eGovernment services offered by them all in one place. It introduces single "*one-place*", "*one stop*" location of hyperlink reference to the list of state and municipal institutions and the eGovernment services which they offer. In order to access the service as such, the individual must first enter the website of the particular institution.

As part of the project Government Electronic Gates – an internet portal of eGovernment services (https://paslaugos.evaldzia.lt/) was launched on 2 June 2006. The users of the system are able to access eGovernment services of various institutions directly through the abovementioned website using uniform authentication means for eGovernment services. In the meantime only a few eGovernment services are accessible through this portal, however the number is increasing.

Local eGovernment

Local eGovernment initiatives are led and coordinated by local authorities – municipalities. Each of them specifies the eGovernment services provided on its own website. Naturally, the number and level of eGovernment services varies across different municipalities. However, overall there are very few interactive services fully rendered in electronic format. For example, the biggest municipality of Vilnius city (www.vilnius.lt) offers only such interactive services as issuance of archive documents of municipality, extracts of municipality documents as well as extracts and copies of documents of liquidated companies or filing of complaints. The order for the abovementioned documents may be filled in on-line, however they are delivered to the requestor in paper form. Authorisation of the user is performed with the help of eBanking authentication means of 7 banks and certificates of the qualified certification services provider – UAB "*Skaitmeninio sertifikavimo centras*".

[9] www.vmi.lt.

[10] www.ivpk.lt.

[11] Informacini• sistem• ir registr• skyrius.

[12] The Department of Inter-Institutional data management (Tarpžinybini• duomen• valdymo skyrius).

Several municipalities set up on-line interactive desks developed by UAB "HNIT-BALTIC" and UAB "Mediaworks" (e.g. municipality of Siauliai city http://e-paslaugos.siauliai.lt/siauliu-e-paslaugos/, municipality of Kaunas http://eps.kaunas.lt:8080/index.do). The users register by filling in their name, surname, personal code, data of passport or personal identity card (together with any information on the legal person and the office held for representatives of legal persons). The more interactive of the eServices of Siauliai municipality require additional authentication via eBanking systems. eGovernment services provided include application for permits to organise public events, filing complaints, applying for permission to take a minor abroad, to get a short time seller's licence for trade in alcoholic beverages etc. The applicant is informed about the results of his/her application via e-mail.

County Government administrations are also launching electronic services projects. In some of them (see www.siauliai.aps.lt) users are authenticated using their usernames and passwords. In order for a user to register, the name, surname, personal identity code and residence address of the natural person residing in a certain county must be provided. Other County Government Administrations are using the authentication mechanism of the Government Electronic Gates, to be accessed via the website of the particular county (see www.klaipeda.aps.lt). The investment project "Installation and Development of Model County Government Administration Information System in the Counties of Lithuania" carried out in 2006 seeks to enable all counties of Lithuania to provide electronic services.

Somewhat harmonizing factor for the municipalities' and counties' electronic services are the requirements for websites of state institutions, set by the Government[13]. Moreover, municipalities and counties are also entitled to provide local eGovernment services via the Government Electronic Gates portal under the same conditions as state institutions.

3.2.2 Traditional identity resources

Authentication towards Lithuanian eGovernment relies on state registers and identity cards. The key registers for the purposes of this study are the Residents' Register, the Register of Foreigners and the Register of Legal Persons.

The Residents' Register (launched in 1992) is the main state register. It contains data of citizens of Lithuania together with the data of persons without citizenship and foreigners declaring their domicile in Lithuania or registering changes in their civil status with the institutions of Lithuania. The register is currently managed by a central institution – Service of Residents Register[14] and its territorial branches (until 2000 it was the Department of Statistics[15]). The territorial branches collect the data and transfer it to the central data base, managed by the Residents' Register Service. The data presently collected includes personal code, other basic personal data (name, gender, date of birth, citizenship), domicile, family status, personal codes of family members, face image, fingerprint, signature etc.

The Register of Foreigners (launched in 2002) contains data on non-citizens. The managing institution of the Register of Foreigners is the Ministry of the Interior; other institutions involved are

[13] Adopted by the Decree No 480 of the Government of the Republic of Lithuania as of 18 April 2003. Bendrieji reikalavimai valstyb• s institucij• interneto svetain• ms, patvirtinti Vyriausyb• s 2003 m. balandžio 18 d. nutarimu Nr. 480.

[14] Gyventoj• registro tarnyba. See www.gyvreg.lt.

[15] Statistikos departamentas prie Lietuvos Respublikos Vyriausyb• s.

the IT and Communications Department under the Ministry of the Interior, Migration Department under the Ministry of the Interior, State Border Guard Service under the Ministry of the Interior[16], Office of the President[17] and Ministry of Foreign Affairs[18]. Apart from the general personal data of foreigners, the Register of Foreigners collects data on illegal stay in Lithuania, procedures of citizenship and asylum, invitation to arrive to Lithuania and visas, issuance of residence permits etc. The Register of Foreigners is connected by reciprocal connection with the Resident's Register.

The Register of Legal Persons (launched in 2004 by way of joining the data on legal persons collected by a number of various state institutions) stores data on legal persons established in Lithuania together with Lithuanian branches and representations of foreign legal persons. The managing institution of the Register of Legal Persons is state enterprise *"Registru centras"*[19]. The information registered varies depending on the type of legal person, but it generally includes the name, legal person's code, place of establishment, legal form, legal status[20], date of establishment, management, economical activity, permits held, branches and representations and any other legally required authentication data.

Access to the information in the Residents' Register and Foreigners' Register is restricted[21], while the Register of Legal Persons is open to the public.

The main identity documents issued in Lithuania are passports and identity cards for citizens[22] and residence permits (temporary and permanent) for non-citizens[23]. The passport was the principal identity document of citizens until 2001 when personal identity cards became the obligatory personal document instead (only as regards the new documents issued). Currently personal identity cards are issued to persons aged 16 and above, and the passport may be issued on additional request[24] and is mainly intended for entries to countries that maintain a visa regime for Lithuanian citizens. Due to this shift some citizens possess both a passport and a personal identity card, others only either a passport or an identity card.

The passport contains data printed on it, namely, first name(s), name, gender, date of birth, place of birth[25], personal code, citizenship, picture[26], signature of the bearer, date of issuance, the issuing institution, period of validity, passport number. The passport remains valid for 10 years.

---

[16] IT ir ryši• depatramentas prie Vidaus reikal• ministerijos, Migracijos departamentas prie Vidaus reikal• ministerijos, Valstyb• s sienos apsaugos tarnyba prie Vidaus reikal• ministerijos.

[17] Prezidento kanceliarija.

[18] Užsienio reikal• ministerija.

[19] See www.registrucentras.lt.

[20] This includes e.g. state of bankruptcy or being wound up.

[21] The person may access data on himself/herself and on other persons provided they possess their permit. Institutions entitled, notaries, bailiffs may access all the data upon separate agreements.

[22] Please also note that special service passport also exists and is issued for certain state servants. The new service passports, issued as of 28 August 2006, hold electronic media for data, see ePassport.

[23] Please note, that foreigner's passport also exists for international travels of non-citizens.

[24] Starting from the age of 18.

[25] Specifically, country name.

[26] The enumerated data is also stored by electronic means in the new ePassports, issued from August 2006. The fingerprints of the bearer shall also be stored by electronic means in the ePassport as of 28 June 2009 following the specifications set by decision of the European Commission No K(2006)2909. Electronic medium, consisting of contactless microprocessor with memory (chip) and antenna is placed in the ePassport. The data recorded is protected with the help of mechanisms of passive authentication and basic access control.

The personal identity card contains first name(s), name, gender, date of birth, personal code, citizenship, picture, signature of the bearer, date of issuance, institution of issuance, period of validity, card number. Personal identity cards are issued for a period of 10 years. The identity cards are of ID1 format under ICAO Doc. 9303 standard (ISO 7810).

Temporary and permanent residence permits for foreigners (EC temporary or EC permanent residence permits for citizens of EC) contain almost the same data as personal identity cards.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The eBanking authentication means

The eBanking authentication means of all nine commercial banks of Lithuania are used for authentication of users of eGovernment services. It should be noted that certain eGovernment applications provide a choice of authentication systems of a few of those banks only. It depends on the agreements with the banks concluded. Only name, surname and personal code of the person held by the bank are used for authentication of users of eGovernment services. The eBanking authentication means are the ones most used by the public sector.

In order to authenticate himself/herself via the eBanking system, the user must first enter the webpage of a certain state institution or the portal Government Electronic Gates and then choose the appropriate bank out of the list. The user is then directed to the webpage of respective bank and prompted to enter username, code (from the codes card or electronic codes generator) and a password. After authentication of the user he/she is asked to consent for the bank to transfer certain personal data (name, last name and personal code) to the Committee, State Tax Inspectorate, municipality or public agency "*Registru centras*", depending on the services requested. Having thus given consent, the user is redirected to the website of the respective institution – provider of eGovernment service or to Government Electronic Gates portal, listing the available eGovernment services. The user may then request the desired eGovernment service.

The electronic authentication means of the banks are usually based on constant user authentication number, code from codes card of ID1 format or electronic codes generator and a password chosen by the user.

The eBanking authentication means are issued by the bank to natural persons only (citizens of Lithuania and foreigners) who have opened bank account with the respective bank and have concluded agreement on electronic services.

Banks are using "Verisign" certificates ensuring the safety of the server. The connection between the internet browser and the bank is protected by Secure Socket Layer (SSL) encryption key.

Personal digital certificates

Personal certificates of 2nd and 3rd class (*see* below the characteristics and definitions of classes) issued by qualified eSignature services providers may be used in a few of eGovernment applications (e.g., submission of financial statements, Government Electronic Gates services).

According to the Lithuanian standard LST ISO/IEC 15408 (original standard ISO/IEC 15408), the certificates management system must conform to security level of at least EAL4 or be in conformity with the standard LST CWA 14167 (original standard CWA 14167).

The complete list of international standards adopted as Lithuanian standards in the field of eSignature and eSignature certificates is available at http://epp.ivpk.lt/lt/apie/standartai/.

Currently there is only one certification services provider issuing qualified certificates in Lithuania registered on 23 February 2005, namely, UAB "*Skaitmeninio sertifikavimo centras*"[27] ("SSC"). Only certificates of this certification services provider may be used for authentication of a person in eGovernment applications as there is no other choice of authentication method using certificates provided in respective eGovernment services websites. Two major Lithuanian electronic communication operators UAB "Omnitel" and UAB "Bite Lietuva" are also planning to provide service of qualified digital mobile eSignature to the public[28].

The certificates may be ordered via certification services provider's website[29] or by filling in the request for certificate and presenting it to registration authority. Either way the applicant must physically present himself to one of the registration authorities for his authentication (this applies to 2nd and 3rd class certificates). In order to acquire a certificate, individuals (either in their own name or on behalf of a legal entity) must present documents proving their identity and other data, to be indicated in the certificate.[30] Registration authorities functions are performed by UAB SSC itself and its authorized registration authorities – companies already performing verification of personal data (such as banks, electronic communication operators) and state institutions.

A few eGovernment applications accepting certificates require either a 2nd or 3rd class personal certificate, issued by a qualified eSignature services provider. The certificate is used for the purposes of authentication of the person only. In order for the certification services provider's certificate to be used, the user must choose the method of authentication – through SSC in the webpage of respective of eGovernment service. If the certificate is stored on a medium (chip card of the dimension of bank card, USB or SIMcard), the user should type in password. In case the certificate is stored in computer, the user should choose the certificate from the list of certificates present in his computer. Both

[27] www.ssc.lt

[28] See www.eparasas.lt.

[29] www.ssc.lt/?name=cert&act=list&L=lt&ssc_mp=3,8.

[30] Article 4.2 of the Law on eSignature.

certificates of 2nd and 3rd class have the functionality of signing with eSignature, however only the certificates of 3rd class are qualified certificates enabling users to sign with eSignature automatically having the effect of handwritten signature.[31]

Usually the digital certificate contains the following data: public key of the holder, name of the holder, the term of validity of the public key, the name of the certification services provider, serial number of the certificate, digital signature of the organisation issuing the certificate.

The certificates may also be used for signing documents of XAdES format under the standard ETSI TS 101 903 v. 1.3.2 XML Advanced Electronic signatures (XAdES) with the help of free software available at http://epp.ivpk.lt/lt/edm/.

Usernames and passwords

A few eGovernment applications authenticate users with the help of identification codes and passwords, either chosen by the user or issued by the provider of the electronic service.

Some applications assign user name upon filling in basic personal information (name, surname, personal code) online. In other cases username and password are sent by e-mail upon conclusion of agreement on data supply via electronic means with the eGovernment service provider – state institution.

Other applications are based on usernames and passwords chosen by users themselves. However, registration to such applications still includes specification of some of the unique identifiers, e.g., name, last name, personal code, passport (or personal identity card) number etc. As regards legal persons, besides the data of the legal person (company name, number etc.) the office held in the entity by the natural person filling in the registration form is required to be indicated additionally.

The eID card

It should be noted that at present electronic eIDs do not exist in Lithuania. The current ID cards only contain visual information and do not posses a chip for storing information. The Ministry of the Interior, Personal Documents' Issuance Centre under the Ministry of the Interior[32] and the Administration of Klaipeda Municipality are currently carrying out the project "Preparation of an Investment Project on the Issuance and the Use of Multifunctional Microprocessor Personal Documents". The aim of the project is to draft an investment project analysing the possibilities to issue a personal document to the Lithuanian residents (and possibly to foreigners – temporary or permanent residence permit) that would participate in the use of eGovernment services.

[31] See Article 8.1 of the Law on eSignature.

[32] Asmens dokument• išrašymo centras prie Vidaus reikal• ministerijos.

It is planned that multifunctional eID cards could be used as means to access and receive public services by electronic means both in Lithuania and the rest of Europe. Moreover, it is anticipated that the eID card would be used for both state and local eGovernment services and private applications.

In the current stage the feasibility study has been conducted for the purpose to examine, inter alia, technical possibilities of implementation of the project. The study envisages application of a multifunctional microprocessor eID card with two independent chips (microprocessors). The first one – contact chip – would enable to install and maintain a few applications and would have the functionality of an eSignature designated to authenticate the users of eGovernment services and to sign electronic documents. The second one – non contact chip – would also enable to install and maintain a few applications, and could ensure the identification of persons and functionality necessary for travel documents as well as the use of eID in applications of additional services (eHealth, eTickets, loyalty programmes, entrance control etc).

It is estimated that in case the project receives the required financing, such eID cards could appear in Lithuania starting from the year 2009-2010.

Inter-institutional data repository

The Inter-institutional tax data repository ("IDR")[33] is a state information system designated to collect tax related data managed by the institutions participating and to supply the data collected to the participating and other institutions. The aim of the IDR is to use tax related data managed by the participating institutions in a more effective way. The participating institutions (they are also the users of the IDR, however other institutions may also become users of the IDR without becoming participating institutions, i.e without supplying the data, e.g. Ministry of Economy) are the following:

- the Ministry of Finance (Finans• ministerija);
- State Tax Inspectorate (Valstybin• mokes• i• inspekcija);
- Customs Department (Muitin• s departamentas);
- Board of State Social Security Fund (Valstybinio socialinio draudimo fondo valdyba);
- Department of Statistics (Statistikos departamentas);
- Financial Crime Investigation Service (Finansini• nusikaltim• tyrimo tarnyba);
- The Committee.

The Committee is the managing institution, which does not upload any data to the IDR. It is important to stress that the IDR is not intended for automatic data supply to information systems of IDR users, but is rather a means for information services provision. Furthermore, only tax related data which does not allow authentication of natural persons may be uploaded to the IDR. The users of IDR may access the data from work places of authorised employees. They may make data requests, save the data received, create their own documents and receive regular standard data. The IDR should ensure more effective data exchange between institutions. The data is collected from information systems of data suppliers and state registers, integrated and arranged according to the needs of IDR users. The IDR is the implementation of Business Intelligence information technologies.

[33] Tarpžinybin• duomen• saugykla. See http://tds.ivpk.lt/.

The data in the IDR is grouped into directories, so called "data windows" (e.g. tax payers, payments and loans, state social security fund data, declarations and reports etc.). The data to be uploaded is sent via e-mail or access to ORACLE database is granted or via FTP.

The System of Registers

The main state registers (there are six of them, e.g. Register of Legal Persons, Residents' Register, Register of Real Estate) together with the related registers (e.g. Foreigners' Register) form the system of registers of Lithuania. The core of the system of registers is their interaction. As regards the system of registers, an "authentic source" principle applies as the data of related registers may not be repeatedly collected from the primary sources and registered. The main registers should be consulted thereabout.

The Register of Legal Persons

The Register of Legal Persons materially contains all basic information regarding legal persons, exercising an economic activity in Lithuania. This basic information includes the official name of legal person, legal form, legal person's code, address of registered office, legal status (e.g. reorganisation, bankruptcy), fields of activity, certain financial information[34], branches and representations, management etc.

All entities in the Register of Legal Persons are identified through a legal entity code. A publicly accessible application[35] allows access to basic information based on the legal entity code (or inversely, to find the legal person's code based on certain information, such as the name of the undertaking).

All information and documents in the Register of Legal Persons are public and rendered upon payment of the respective fees, as established by legal acts. A full search on legal persons in the electronic data base of the Register of Legal Persons is possible upon agreement on data supply with the register (such method of access to data is only available for legal persons[36]). Having concluded an agreement on data supply, a legal person may access the data of the Register of Legal Persons from his own computer by entering the granted username and password. The user may see the data on legal persons together with entries of documents submitted to the register. In order to receive any document regarding a legal person, an additional request must be made and the copy is delivered in paper form.

Authentication policies

There is no official authentication policy in Lithuania that defines a strict hierarchy of the different authentication systems in use. The Position Paper on eGovernment only declares that system of

[34] e.g. share capital for limited liability companies, dates of financial reporting etc.

[35] The so called Public Search; see http://www.registrucentras.lt/jar/paieska/.

[36] See http://www.registrucentras.lt/jar/registracija.php.

authentication of residents in information systems should be created for administration of public services. The Position Paper also provides for the operation of eGovernment projects regardless of the eSignature infrastructure in Lithuania. Other alternative means to ensure safety and to authenticate users may be applied where authentication of the user and safe connection between the user and the server are ensured. Based on this provision one may deduce that the eSignature is the highest level of authentication. However, in practise each eGovernment application has its own semi-autonomous authentication system which is considered to be of a sufficient level and has no superiority as regards other authentication systems of other applications.

As regards the Government Electronic Gates portal both eBanking authentication means and personal certificates are considered have the same effect for user authentication.

However, it should be noted, that as a rule more interactive services require eBanking authentication means or passwords rendered by the eGovernment service provider whereas passwords chosen by user do not suffice.

3.3.2 Legal framework

The main legal acts for eIDM systems:

- Resolution No 2115 of the Government of the Republic of Lithuania on Position Paper on eGovernment as of 31 December 2002[37];
- The Law on Electronic Signature No VIII-1822 as of 11 July 2000[38];
- Order No T-127 of the Director of the Information Society Development Committee adopting the Rules on Functioning of Government Electronic Gates when Providing eGovernment Services as of 30 December 2005[39];
- The Law on State Registers No I-1490 as of 13 August 1996[40] ;
- The Law on Passport No IX-590 as of 8 November 2001[41];
- The Law on Personal Identity card No IX-577 as of 6 November 2001[42]

---

[37] 2002 m. gruodžio 31 d. Vyriausyb• s nutarimas d• l elektronin• s valdžios koncepcijos patvirtinimo Nr. 2115; See http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198184&p_query=&p_tr2=;

[38] 2000 liepos 11 d. Elektroninio parašo •statymas Nr. VIII-1822; See http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=169880;

[39] 2005 m. gruodžio 30 d. Informacin• s visuomen• s pl• tros komiteto prie Lietuvos Respublikos Vyriausyb• s direktoriaus •sakymas d• l Valdžios elektronini• vart• funkcionavimo teikiant vieš• sias elektronines paslaugas taisykli• patvirtinimo Nr. T-127;See http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=268958&p_query=&p_tr2=;

[40] 1996 m. rugpj• • io 13 d. Valstyb• s registr• •statymas Nr. I-1490;See http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=238968;

[41] 2003 m. lapkri• io 8 d. Paso •statymas Nr. IX-590; See http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=280169;

[42] 2001m. lapkri• io 6 d. Asmens tapatyb• s kortel• s •statymas Nr. IX-577; See

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=154166&p_query=&p_tr2=;

Other relevant legislation:

- Government Resolution No 1346 Approving Statutes of the Residents' Register as of 6 November 2000[43];
- Government Resolution No 1407 on Establishment of the Register of Legal Persons and Approval the Statutes thereof as of 12 November 2003[44];
- Government Resolution No 1049 on Establishment the Foreigners' Register and Approval the Statutes Thereof as of 4 September 2000[45];

Lithuania has no specific regulations with regard to the process of authentication in general. The provision of the Position Paper on eGovernment stating that other means to ensure safety and to authenticate users may be applied (apart from the eSignature) where authentication of the user and safe connection between the user and the server are ensured, is the basis for eGovernment applications, relying on user authentication.

The 'Rules on the Functioning of the Government Electronic Gates when providing eGovernment services' is the only document describing user authentication applicable to a group of applications. It states that authentication of users via the Portal is made through a chosen eBanking system.

As regards future legislation contemplated, it is planned to adopt a Law on State Information Resources Management. The conception of the Law[46] has already been adopted putting forward the principal guidelines. The anticipated law would stipulate unified standards in order to use the state's information resources more efficiently and to ensure interoperability between different databases. As a result the law should contribute to smoother exchange of data among state institutions and provision of eGovernment services following the "one-stop" principle[47].

Electronic authentication systems are not mandatory as the electronic method is complementary to paper forms based method of rendering public services.[48]

---

[43] 2006 m. lapkri•io 6 d. Vyriausyb•s nutarimas Nr. 1346 d•l Lietuvos Respublikos gyventoj• registro nuostat• patvirtinimo; See

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=273204;

[44] 2003 m. lapkri•io 12 d. Vyriausyb•s nutarimas Nr. 1407 d•l Juridini• asmen• registro •steigimo ir Juridini• asmen• registro nuostat• patvirtinimo; See

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=291860;

[45] 2000 m. rugs•jo 4 d. Vyriausyb•s nutarimas Nr. 1049 d•l Užsienie•i• registro •steigimo ir nuostat• patvirtinimo; See

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=268107;

[46] Government Resolution No 1367 on approval on state information resources management conception as of 29 December 2006. 2006 m. gruodžio 29 d. Vyriausyb•s nutarimas Nr. 1367 d•l Lietuvos Respublikos valstyb•s informacini• ištekli• valdymo •statymo koncepcijos patvirtinimo; See

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=289797&p_query=&p_tr2=;

[47] i.e. accessible from one point of entry.

[48] Except for Customs declarations via NCTS where electronic means is the only possible and binding method.

The definition of eSignature,[49] provided in the Law of Electronic Signature identifies two functions of eSignature: confirming the authenticity of data and (or) authentication of the signatory. As a matter of practice, the legal framework distinguishes between signatures and mere authentication.

Access to the information in eIDM systems is provided to the institutions specifically granted such rights by virtue of legal acts: institutions managing the eIDM systems, providing public services based on the data etc. Private persons are entitled to access to information stored in registers about themselves. Data held by the Register of Legal Persons is accessible to the public. Legal persons may even access electronic databases of the register upon special agreements on data supply with the register[50].

As mentioned above, the data of the Register of Legal Persons may be used by private legal persons. It is also anticipated that the eID cards would also have the functions allowing installation of private applications. Inversely, the portal Government Electronic Gates may only be used by public entities – providers of eGovernment services. Private entities may not render services via this portal.

Under the Law of eSignature[51] the power of the eSignature of a representative of legal person is given the same recognition as that signed by a representative of the legal person, confirmed by the stamp of the legal person, appearing in written documents, taking into account the power of the eSignature. As a general rule natural persons authorised to represent legal persons electronically are specified by the legal person in the agreement with respective provider of eGovernment services. However, please note that authentication of legal persons is not available in all eGovernment applications.

The use of the personal code granted by the Residents' Register is only allowed upon permission of the data subject. The derogations from this rule include purposes of management of state registers and information systems as regulated by legal acts.[52]

3.3.3 Technical aspects

Digital personal certificates

Technical specifications of the certificates issued by UAB "*Skaitmeninio sertifikavimo centras*":

[49] Electronic Signature means data, which are inserted, attached to or logically associated with other data for the purpose of confirming the authenticity of the latter and (or) authentication of the signatory. (Art. 2 of the Law on Electronic Signature).

[50] See www.registrucentras.lt/jar/registracija.php.

[51] Article 8 part 4.

[52] See. Art 7 of Law on Legal Protection of Personal Data as of 11 June 1996 No I-1374. 1996 m. birželio 11 d. Asmens duomen• teisin• s apsaugos •statymas Nr. I-1374.

Certificate standards **X.509 v3 (including all extensions)**
- PKIX
- SSL
- S/MIME
- IPSec
- SET

Certification
Common Criteria EAL4+

Features of certificates catalogue
LDAP v.3 certificates repository

PKI features
Real time verification of the status of certificates via OCSP responder
X.509 Certificates Revocation Lists (CRL)
Multiple levels of CA (sub-CA)

Certificates features
X.509 v1, v3 certificates
RSA and DSA crypt algorithms
Key size up to 2048 bits
Flexible DN configuration
Compatibility with Netscape® Communicator and Microsoft® Internet Explorer

Cryptographic support
- RSA
- DSA

Devices for decryption
CA private keys held in PKCS #11 devices
FIPS 140-1 level 1 to level 3 key protection (with the help of nCipher and/or Chrysalis)

Cryptographic API
•PKCS#11 v1 and v2.01
• Microsoft CryptoAPI v2.0
• JCA (Java Cryptographic Architechture)
•OpenSSL

Classes of certificates[53]:

[53] All information on the classes of certificates and their profiles is from the Certificate Practices Statements of UAB "Skaitmeninis Serifikavimo Centras" (ver. 1.0.0 [LT]) and from the following website www.ssc.lt/?name=menu_p&act=show&do=3,35&L=lt.

1st class certificate

The profiles of 1st class certificates are in conformity with the standard RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

2nd class certificate

The profiles of 2nd class certificates are in conformity with the standard RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

3rd class certificate

At least the main fields of the first version X.509 and values set in advance together with the restrictions of values, indicated in the table below, must be present in the certificates X.509 issued by SSC:

Qualified 3rd class certificate				
Base Certificate	**Include**	**Critical**	**Value**	
signatureAlgorithm	X		SHA-1 with RSA Encryption	Fixed
signatureValue	X			
tbsCertificate				
Version	X		2	
SerialNumber	X		Provided by RA	Dynamic
Signature	X		SHA-1 with RSA Encryption	
Validity				
NotBefore	X		Key Generation Process Data/Time	
NotAfter	X		Key Generation Process Data/Time + 2 years	
SubjectPublicKeyInfo	X		RSA 1024	
Issuer				
CountryName	X		LT	Fixed
CommonName	X		3rd class certificate	Fixed
Subject		Required		
countryName		YES	LT	Dynamic
CommonName		YES	Given name, surname, serial number – provided by RA	Dynamic
Surname		YES		Dynamic
GivenName		YES		Dynamic
NickName		YES		Dynamic
AlternativeName				
serialNumber		YES	Provided by RA (11 digits value)	Dynamic
Representation		Required		
Name of legal entity, code		YES	-	
Address			-	
Rights of representation		YES	- The rights of the signatory to act on behalf of legal entity; - The scope of empowerments;	

			- The grounds of empowerments; - Term of empowerments.	
Standard Extensions	Include	Critical	Value	
CertificatePolicies			CP	
policyIdentifyer				Fixed
policyQualifiers			N/a	
policyQualifierId	X		EuroPKI Certificate policy OID 1.3.6.1.4.1.5255.1.1.1 (Version 1.1).	Fixed
Qualifier	X		http://www.ssc.lt/	Fixed
Qualified Certificate Statement				
QcStatement	X			
Key Usage	X	TRUE		
nonRepudiation			Set	Fixed
authorityKeyIdentifier	X	FALSE		
KeyIdentifier	X		SHA-1 Hash	
cRLDistributionPoints	X	FALSE		
distributionPoint				
Basic Constrains				
Signatory			End user	
Enhanced Key Usage				
NetscapeCertType	X	FALSE		
Private Extensions	Include	Critical		
AuthorityInfoAccess	X	FALSE		
Destination Restrictions / monetary value				

The eID card

Under the feasibility study the anticipated eID card would be a multi-application card for electronic authentication and MRTD with biometric data authentication verification. The eID card would contain two separate embedded chips (microprocessors):

- the first chip – contact (under ISO 7816-2 [59]) with possibility to install and maintain a few applications (multi-applicational). This chip shall conform the requirements of storing PIN and biometric data;

- the second chip – contactless (under ISO 14443 [68-]) with possibility to install and maintain a few applications (multi-applicational). This chip shall conform to the requirements of media structures maintenance and the biometric data.

The visual data on the surface of the eID card shall not be different from the present personal identity cards and the format of the eID card should remain the same ID1.

On-card applications

The main applications to be installed in the eID card are:

PKI application (under PKCS#15) or eSignature application, designated to ensure authentication of users of eGovernment services (electronic authentication with protection provided by PIN or biometric data) and to electronically sign documents. Application installed in contact chip.
ICAO LDS format MRTD application for reliable physical authentication, the same as in ePassport. Application installed in contactless chip.

Additional post-issuing applications include:

1. Applications containing any identifying or confidential data of the card holder (e.g., ePrescription, ePatient's card) may be installed on (and uninstalled from) the contact chip;
2. Applications containing no identifying or confidential data of the card holder, but requiring minimal cryptographic protection (DES numbering algorithm and/or eSignature) (e.g., transport eTickets, discount cards for goods and services, social concessions, entry control) may be installed on (and uninstalled from) the contactless chip.

3.3.4 Organisational aspects

The investment project "Interoperability of information systems of public administrations – creation of system's interoperability capacity" is being implemented by the Committee, department of Inter-institutional data management[54]. The aim is to create a unified technological platform enabling data interchange among state registers and information systems. Such interoperability would allow the application of a "one-stop" principle. All subjects participating in the provision of eGovernment services would use the unified data exchange format and integration interface in order to take data from different sources, to process the data and to provide eGovernment services.

The Government Electronic Gates portal (https://paslaugos.evaldzia.lt/) is the central (state) portal of eGovernment services created while implementing the abovementioned investment project. It performs the function of intermediary between eGovernment services providers and users and operates as a front-office. The portal performs user authentication, authorisation, identification of the request and transfer thereof to the institution – service provider (back-office), control of the process and presenting the result to the user. The Government Electronic Gates portal ensures central authentication of users.

The main emphasis is placed on the 20 eGovernment services recommended by the EU. However, it should be noted that some of the eGovernment services (e.g. submission of tax, customs declarations, financial reporting) have their own authentication mechanisms and are provided via the websites of their respective institutions. It is not anticipated to put those mechanisms in the

[54] Tarpžinybini• duomen• valdymo skyrius.

Government Electronic Gates portal, however, the data held by those institutions could be used when providing eGovernment services of other institutions via the Portal.

The provision of eGovernment services not attributed to a particular institution via the Portal is also anticipated together with complex services, composed of the eGovernment services already provided.

The Portal was launched on 2 June 2006. The users of the system are able to access eGovernment services of various institutions directly through the abovementioned website using uniform authentication means for all eGovernment services. The Department of inter-institutional data management of the Committee is the manager of the Portal. As of 16 April 2007 the following 5 eGovernment services are available at the Portal:

- checking of the contributions paid by the employer to the State Social Security Fund Board[55];
- checking the medical services rendered and the medicaments prescribed;
- delivery of documents to Communications Regulatory Authority[56] by electronic means;
- order and payment for certificate on declared place of residence;
- order and payment for certificate on family situation.

The Central Mortgage Office[57] and State Road Transport Inspectorate[58] are also planning to provide eGovernment services via the Government Electronic Gates portal in the near future.

User authentication is currently only available for natural persons. The possibility to authenticate legal persons is under consideration, with the view to be able to authenticate legal persons via the Portal starting from the end of this year. Natural persons are authenticated using eBanking authentication means or a personal digital certificate of 2nd or 3rd class, issued by a qualified eSignature services provider (discussed in more detail above). The data held by the bank or UAB "*Skaitmeninio sertifikavimo centras*", such as name, surname and personal code of the person, are used for authentication. Any other information held by the bank or certification services provider (e.g. accounts, transactions etc.) is not supplied from the bank's or certification services providers' system.

As mentioned above, some eGovernment applications (e.g. tax, customs declarations, financial reporting, local eGovernment services) have their own eIDM systems, due to the sector based approach of eGovernment services from the beginning. However, those systems are also based on eBanking authentication means, personal certificates or passwords and codes.

3.4 Interoperability

[55] Valstybinio socialinio draudimo fondo valdyba.

[56] Ryši• reguliavimo tarnyba.

[57] Centrin• hipotekos •staiga.

[58] Valstybin• keli• transporto inspekcija.

The eBanking authentication means are available for foreigners who have opened accounts with the appropriate banks, and personal certificates of 2nd and 3rd class may also be issued to foreigners.

The contemplated electronic temporary and permanent residence permits should also be issued to foreigners according to the feasibility study on eID cards.

Furthermore, the interoperability of the anticipated eID cards with the European systems is foreseen. The eID card should comply with the ECC standard [51-55]. A project of technical specifications has been prepared, ensuring interoperability with standard equipment: card readers, terminals, PC-based user applications etc.

In contrast, no noteworthy initiatives have so far been taken to enable the use of foreign eID cards or other user authentication means in Lithuania.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

3.5.1 eBanking authentication means applications

Outside of the eBanking sector, eBanking authentication means (usernames, codes cards and generators, passwords) are used in the following main public sector applications:

- Electronic Tax Declaration System (EDS) http://deklaravimas.vmi.lt;
- Government Electronic Gates applications https://paslaugos.evaldzia.lt/;
- Electronic Services of State Enterprise Centre of Registers System (CEPS) www.registrucentras.lt/ceps/;
- A variety of local services (see above).

3.5.2 Personal certificates of 2nd or 3rd class

Personal certificates of 2nd or 3rd class issued by SSC are used as authentication means in the following main public sector applications:

- Electronic Tax Declaration System (EDS) http://deklaravimas.vmi.lt;
- Government Electronic Gates applications https://paslaugos.evaldzia.lt/;
- Electronic Services of State Enterprise Centre of Registers System (CEPS) www.registrucentras.lt/ceps/;
- A few local services (e.g., www.vilnius.lt).

The certificates may also be used when signing documents with an eSignature.[59]

3.5.3 Usernames and passwords

Usernames and passwords created by the users are used in the following public applications:

- Public procurement http://www.cvpp.lt/;
- A variety of local services (see above).

Usernames and/or passwords granted by the public service provider are used in the following public applications:

- Electronic Tax Declaration System (EDS) http://deklaravimas.vmi.lt;
- Statistical reports submission https://e-formos.stat.gov.lt/alfa/AW/registracija;
- Preliminary registration within the State Labour Exchange http://www.ldb.lt/WWWAnketa/index.aspx?psl=epaslauga;
- Access to the data of Register of Legal Persons https://jar.registrucentras.lt/paieska/;
- Access to the data of Residents' Register http://www.gyvreg.lt/;
- Submission of Transit Declarations through NCTS http://www.cust.lt/lt/rubric?rubricID=264.

3.5.4 eID card applications

It is anticipated that the eID card could be used in future in the following public and private sector applications:

- eTickets in public transport;
- eHealth applications (ePresciption, ePatient's card etc.);
- social security applications;
- entrance control applications (in offices, libraries etc.);
- eLoyalty programs (discount cards).

3.6 Future trends/expectations

As regards the existing systems, it is likely that in the future the number of eGovernment services (including the ones accessible via the portal Government Electronic Services and based on the existing authentication methods) will increase together with the number of the institutions – users of

[59] Free software program may be used for signing available at http://epp.ivpk.lt/lt/edm/.

the Inter-institutional data repository. Furthermore, electronic authentication means should become accessible to legal persons in the Portal.

In the field of the new projects, as has been already mentioned, the most significant of the eIDM systems is the possible introduction of an eID card (see more in the previous chapters) performing both the physical and electronic authentication of persons and having the functionality of fully-fledged eSignature.

Besides that, the project on the establishment of the State Data Management Centre has been launched recently. The project should contribute to the implementation of "one-stop" principle as one platform of management of data flows between state institutions and between institutions and society will be created. The Centre will be responsible for the administration of the eGovernment portal. The new Department of inter-institutional data management of the Committee[60] will manage this State Data Management Centre. The centre will only provide access to data, but will not contain any data on subjects itself. The provision of all eGovernment services should eventually be based on the use of the eSignature and all eGovernment services should be accessible from one point. It is anticipated that it should also be possible to order eGovernment services using a mobile phone.

Furthermore it is also anticipated to issue civil servant identification cards with eSignature data (keys, certificates stored in cards with chips) starting from 2007-2008. The Committee would act as certification authority.

The cooperation of the public and private sector is most evident in the form of "eSignature Breakthrough Programme"[61]. It is the project initiated by the Government of Lithuania, the leading electronic communication operators and banks, aiming to harmonize technological solutions and to offer services using an advanced eSignature based on PKI technology to the mass market starting from the year 2007. The means to achieve the said aim include agreements on common standards, launching of pilot projects for use of advanced eSignatures in commercial sector, information campaigns on eSignature, state aid to the citizens in acquiring advanced eSignature equipment, providing state institutions with advanced eSignature equipment, etc.[62] It is anticipated that residents will be granted the possibility to change their SIM cards of mobile phones to the new ones, performing functions of SMART cards in the eSignature infrastructure.

3.7 Assessment

The actual use of the country's eIDM infrastructure depends directly on the number of interactive eGovernment services available. The most successful eGovernment application – submission of tax

[60] Established as of 1 January 2007.

[61] See more about the programme at www.parasas.lt.

[62] The "eSignature Breakthrough Programme" may be found at http://epp.ivpk.lt/epp/Dokumentai/2006-10-18%20E.paraso%20proverzis.pdf.

declarations via electronic means[63] – results in the popularity of the authentication means used in this application. As the number of eGovernment services increases, it is likely that the eIDM infrastructure will also develop alongside.

3.7.1 Advantages:

- The reliance on eBanking user authentication system worked out smoothly and satisfies the present relatively low level intensity of eGovernment services. Main eGovernment applications have agreements with all 9 commercial banks operating in Lithuania and offering eBanking services and are thus available to all users of eBanking regardless of their bank.
- The existing system is rather simple for users as it relies mostly either on already familiar eBanking authentication system and means or either on simple passwords and codes combination. The personal certificates are not widely spread and used only by more advanced users.
- The system in principle does not discriminate foreign entities as compared to Lithuanian ones.

3.7.2 Disadvantages:

- Due to relatively low number of completely interactive eGovernment services accessible the use of the eIDM systems is not that high.
- No universal state eIDM system or infrastructure is present. The state relies on private structures. As a result the users of eGovernment services must trust eBanking as such in order to request public service. Furthermore, such authentication means are only available for natural persons who have opened account with the respective bank and concluded agreement on provision of electronic services and are not yet available to legal persons in some applications.
- Sector based approach from the outset of the eGovernment services lead to separate applications using different authentication mechanisms and having their own websites as front-offices.
- Other private applications may not be installed in the present eIDM schemes used for public services.
- Authentication mechanisms do not ensure functionality of eSignature (except for personal digital certificates of 3rd class).
- No universal data exchange platform between institutions exists enabling the real application of “one-stop” principle.
- Interoperability is not ensured with the other eIDM systems across the EU.

Contact persons:

[63] According to the data of State Tax Inspectorate 46% of residents submitted their tax reports for the year 2005 via electronic means. At the meantime 64% of legal persons submit their tax returns electronically. See www.vmi.lt/lt/?itemId=10135415.

Name	Tel. No	E-mail	Institution	Subjects
Martynas Jok• bauskas	0037052665189	m.jokubauskas@ivpk.lt	Department of inter-institutional data management of the Information society development Comittee	Data Management Centre, Inter-institutional data repository
Tomas Sakalauskas	0037052665184	t.sakalauskas@ivpk.lt	Department of Inter-institutional Data Management of the Information Society Development Comittee	Portal Government Electronic Gates
Almantas Buitkus	0037052663836	a.buitkus@ivpk.lt	Department of IT Systems and Registers	Registers
Aušra Ka• inskien•	0037052717379	ausra.kacinskiene@vrm.lt	Section of eGovernment services of the Department of Information Policy under the Ministry of the Interior	eID cards