eID Interoperability for PEGS

NATIONAL PROFILE SLOVAKIA

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 Slovakian 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 contrd; 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

In Slovakia, there is no general eIDM system. If the administrative body wants to use identity management in electronic form, it has to establish ad hoc a new eIDM system.

Thus, an eIDM system based on eID cards as a mandatory electronic identity card intended to facilitate access to eGovernment services is currently not in operation. There are a few strategies, including plans for the introduction of eID cards.

The most significant eIDM system in Slovakia based on the Slovakian eID Card with a chip card and qualified electronic signature will be introduced according to the task No. 10 of the Action Plan Minerva[3] by the end of the next year. Before this is done, it will be necessary to introduce an identifier for the communication between information systems of public administration that will be unique, and to generate a unique personal identifier from the birth number.

According to the data protection law the current birth number[4] is not usable for the information systems of public administration because it is possible to derive from it the personal data of the person, such as date of birth, sex, place of birth etc. But the birth number is currently used in all public sector systems and unfortunately, many Slovakian laws are explicitly bound up with the birth number. From that reason the replacement of the "old" birth number by a new unique identification number will be a long process and probably both numbers will be used for a few years simultaneously.

Sometimes, qualified certificates issued by accredited certification authorities are used in connection to eIDM. But it is not allowed to state the birth number of a natural person in a qualified certificate, and because of the present lack of another unique personal identifier it contains no clear unique personal identification data that would enable to uniquely identify the natural person. This seems to be the biggest issue; if the citizen wants to use the qualified certificate to sign electronically in communication with public administrations, that issue is actually solved by prior physical authentication.

Public usage statistics for any eIDM system are currently not available and such numbers are not yet processed by the Statistical Authority of the Slovak Republic. All qualified certificates have to be issued on secure signature creation devices (mandatory) – on tokens, smart cards etc. The actual number of issued valid qualified certificates is around 4.000 (official statistics are not available; this figure is only the estimate of the supervisory body for electronic signatures), but the expected

[3] Short name of document „*Strategy of Development an Information Society under conditions of SR and the Action Plan"* adopted by Government of the Slovak Republic and describing the process of developing an electronic public administration.

[4] The birth number can be used in paper form only.

evolution is many times higher. After the introduction of the ID card including a chip and qualified certificate, its penetration is expected for all adults.

All of the eIDM systems will be discussed in greater detail below.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

In Slovakia there were many attempts to establish a form of centrally coordinated eGovernment. But in reality, eGovernment consists of many applications developed in different ways and by different public administration bodies and this process cannot be considered a centralized model. The only measure taken to coordinate the application developed by resort was the establishment of the Central Public Administration Portal, from which all services are accessible (but all those application use different technical environments[5], have different identification systems of the users etc.).

According to the amendment of the Act of the National Council of the SR No 575/2001 Coll. on the organisation of activity of the government and organisation of the central state administration entered into force and effect since 1 February 2007, the central body of state administration for the building of the information society is the Ministry of Finance of the Slovak Republic and partly Governmental Office of the Slovak Republic. Besides them the National Security Authority as a central state administration body is responsible for information security and for electronic signatures. The general regulation of the position of the Ministry of Finance in the area of the building of the information society is stipulated in detail by the act on information systems of public administration and on amendments of certain Acts[6].

Moreover, the Ministry of Transport, Post and Telecommunication issues and declares standards that are very important from the view of the achievement of the interoperability of information systems of public administration. We regard this regulation of the position of the MTPT SR as sufficient and cost-optimal from the view of providing for the coordination of an eGovernment development.

The use of eIDM systems in the context of eGovernment is not well coordinated. The introduction of a planned central eIDM system through eID cards has already taken a long time, and to no tangible effect. In the past years, several eGovernment applications have been developed, but none of them on the central level. The only step taken to coordinate eGovernment development was the building of the Central Portal of the Public Administration, from which all those services should be accessible. At this moment all applications use different ways of user authentication.

[5] The reason is very general character of standards for information systems of public administration and this kind of regulation seems to be unsufficient for the interoperability.

[6] Act of 20 April 2006 No. 275/2006 Coll. on information systems of public administration.

3.2.2 Traditional identity resources

The main IDM system traditionally used in Slovakia is the Population Register[7]. The Population Register, managed by the Ministry of the Interior[8], is a part of the state information system, that includes a set of information on the Slovak Republic citizens based on which it is possible to identify a person, to find out his/her residence and his/her relations to other persons. It is used as a source of valid information on the Slovak Republic citizens for the needs of the state administrative bodies, territorial self-government bodies, and other legal or natural persons.

The Population Register includes information on following groups of persons:
a) citizens with permanent residence in the territory of the Slovak Republic;
b) citizens who do not have permanent residence in the territory of the Slovak Republic;
c) foreigners reported for a stay in the territory of the Slovak Republic;
d) foreigners who were granted asylum within the territory of the Slovak Republic.

The register contains identity information including personal data (name, surname, academic title, maiden name, birth number, date of birth, place of birth, district of birth, country of birth, sex, family status, nationality, date and place of death), information on permanent or temporary residence (name of district, name of community, name of the part of the community, name of street, orientation number, register number), information on relationship to other persons (personal data of husband or wife, personal data of father and mother, personal data of child) and administrative information on the person (number and series of identification card, number and type of travel document, if issued, information on the court's decision related to the capability for legal acts, information on the court's decision related to the divorce of marriage, information on the court's decision related to the announcement that the marriage is invalid, information on the court's decision related to the announcement that the Citizen is dead, information on the ban of the stay, information on the granting of the Slovak Republic nationality).

The main identifiers of a natural person traditionally used are the personal identification number (so called "birth number" – "*rodné • íslo*"), the computer number from the information system of population register, the tax identification number (I• O), and identifiers from information systems of the social security register or health register.

The birth number is used as primary identifier that uniquely identifies personal data. The creation of the birth number, its allocation, the administration of the Birth numbers register and any other useful information are laid down in the Birth Number Law[9]. This number (as a permanent and primary

[7] Act No. 253/1998 Coll. On the notification of citizen residency and on the population register of the Slovak Republic. English version available on http://www.civil.gov.sk/documents/p07-f02.doc

[8] Information and forms available on http://www.civil.gov.sk/p07/p07.shtm .

[9] Act No. 301/1999 Coll. on the birth number. (Also English version available: http://aprox.government.gov.sk/iap/aprox.nsf/0/88E73610A13EA4CAC1256DB4003B22AA?OpenDocument)

identifier) is registered in the central population register managed by the Ministry of Interior (mentioned above). The birth number is allocated by the Register Office (*Matri• ný úrad*) after birth to every person born on the territory of the Slovak Republic. Until now, not all Register Offices are connected to the central Birth number register, which caused a few problems in their management. In the year 1995 we noticed 60.000 instances of duplicate birth numbers (the same birth number for two or more persons); today we estimate the number at 30.000.

The Ministry of Interior through the Register Office assigns the birth number to citizens born in the territory of Slovak Republic with permanent residence in Slovakia, to citizens of the Slovak Republic born abroad, to foreigners with permanent or long-term residence in Slovakia, to refugees[10] residing in Slovakia and to person without residence in Slovakia, who applied for it

The birth number for a person born until 31 December 1953 has nine figures, and ten figures for a person born after 1 January 1954.

While many Slovakian laws are explicitly bound up with the birth number, it is none the less not usable for the information systems of public administrations because it is possible to derive from it from the personal data of the person, such as date of birth, sex, place of birth etc. This issue together with the issue of duplicate birth numbers (the same birth number for two or more persons – which can be rectified on the basis of application) caused that already in the year 2006 the Ministry of Interior planned to replace the old system of creation of the birth numbers by a new system. There were a few initiatives (JIFO, BIFO etc.) using a cryptographic algorithm. It was also planned to enable the online connection between different existing national registers. But the replacement of the "old" birth number by a new unique identification number will be a long process and probably both numbers will be used for a few years simultaneously.

The document formally stating the birth number is either the birth certificate or identity card, travel document (passport), residence permit or confirmation on birth number. In practice the identity card is primarily used for authentication.

The identity card is issued to all citizens after they reach the age of fifteen (mandatory) or get the citizenship of the Slovak Republic or for the people residing in Slovakia. The current identity card is usable in paper (physical) form only, but there are a few initiatives (such as the Action Plan Minerva), that plan to introduce an eID Card with a chip card and qualified electronic signature.

The current (paper based) ID cards are issued for period of 10 years (for persons over 60 the validity is unlimited). It contains the ID card number, personal data of ID card holder (name, surname and maiden name, birth number, date and place of birth, sex (gender), citizenship, and permanent residence address), date, expiration and place of issuance and machine readable text. Furthermore, there is a picture of the bearer and a few security components and a space for special data (such as academic title, blood group etc.). The content of the residence permit is similar to the identity card.

Information regarding legal entities is not centralised in one register, but is rather spread over two main registers: the Trade register and the Commercial register.

[10] Act No. 283/1995 Coll. on refugees.

The Trade register (*Živnostenský register*[11]) is managed by an organisation which is part of the Ministry of Interior. Information regarding entrepreneurs in the register is maintained by ObÚ (*Obvodný úrad, odbor živnostenského podnikania*), where the entrepreneur is registered. Finding an entrepreneur in the trade register is possible according to I• O number (identification number of business entity), company name (according to company name or the address of the business), surname and name of physical entity (according to surname and name, or address of company) or according to address of establishment. In spite of electronic management of this register, a trade licence in electronic form is currently not usable for legal acts.

The Commercial (companies) register[12] is managed by the Ministry of Justice. Any application to the registration court must be filed on a specific form issued by the Ministry. If an application is accepted, the relevant facts are registered with the Commercial Registry within five days from the date of the application. A statement on registration, together with an extract from the Commercial register, is issued and delivered to the applicant free of charge. In spite of the electronic management of this register, the extracts from the Commercial register in electronic form are currently not usable for legal acts, but from 1 August 2007 it will be possible to file an application for a registration into a Commercial register electronically signed by a qualified electronic signature and to issue the outputs in electronic form signed by qualified electronic signature. But the filing of an application requires a so called pairing of the physical identity with an electronic identity (with certificate) either through the central portal of the public administration or directly through the court (the main reason is a lack of unique identifiers for natural persons and the impossibility of using birth numbers in qualified certificates).

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

In Slovakia, there is no general eIDM system. If an administrative body wants to use an electronic identity management system, it has to establish a new ad hoc eIDM system. An eIDM system based on eID cards as a mandatory electronic identity card intended to facilitate access to eGovernment services is currently not in operation. There are a few strategies planning the introduction of eID cards.

The most significant national strategies adopted by government include the plan to introduce a central eIDM system. An eIDM system based on the Slovakian eID Card with a chip card and qualified electronic signature will be introduced according to the task No. 10 of the Action Plan Minerva[13] by the end of the next year. Before this can be done, an amendment of the Identity Cards Law is needed. According to a document from the Ministry of the Interior named “The possibilities of an introduction of electronic identification cards”, these should replace today’s paper based identity cards

[11] Act No. 455/1995 Coll. On trade enterprise (http://www.zrsr.sk – also English version available)

[12] From 2 February 2004 proceedings at the Commercial Registry are no longer regulated by the Commercial Code. Such proceedings are now subject to Act No. 530/2003 Coll. on the Commercial Registry (the Commercial Registry Act). The whole process concerning the registration of information has been streamlined.

[13] Short name of document „*Strategy of Development an Information Society under conditions of SR and the Action Plan”* adopted by Government of the Slovak Republic and describing the process of developing an electronic public administration.

and should include a chip with a qualified certificate and an authentication certificate. They will be issued to persons from 15, but the chip will only be included if the person will apply for it. Otherwise they will receive only the polycarbonate card with data and a picture. However, the chip on the eID card will be empty (there is no state CSP issuing qualified certificates currently); if the eID card holder wants to have a private key and qualified certificate on it, he has to buy it from accredited commercial CSPs. Before this is done, it is also necessary to introduce an identifier for the communication between information systems of public administration that will be unique (task No. 7 of the Action Plan Minerva[14]). The tasks of the Action Plan Minerva are specific projects directly tied to the Action Plan of the Information Society Strategy and with recommendations of the Lisbon Action Programme.

As will be mentioned further below, in Slovakia there is no special legal framework for authentication, and until now no central infrastructure has been built.

In general, in Slovakia 3 systems (levels) are commonly used for identification/authentication purposes in electronic communication:

Basic user name and password

Authentication through the username and password is used in the Central Portal of Public Administration.

Qualified certificates and registration process

Sometimes in connection to eIDM qualified certificates issued by accredited certification authorities are used. But it is not allowed to state a birth number of natural person in a qualified certificate, and because of the present lack of any other unique personal identifier it contains no unique personal identification data that would enable to identify the natural person. This seems to be the biggest issue; if the citizen wants to use the qualified certificate to sign electronically in communication with public administration, that is actually solved by prior physical authentication (e.g. in eServices of the Commercial Register, eTax etc.).

eTax services (electronic tax returns) for individuals as well as eTax and eVAT services for businesses have been available since 2004. To access these services, a user needs either a qualified certificate from an accredited CSP or a password. For eTax in general, prior to first usage a registration procedure at a local tax authority is required. During this registration process, the identity of a user is proven by using conventional identity cards. After the initial procedure, the user can access his tax account. The prior physical authentication is necessary because the qualified certificate does not contain a unique identifier of natural person (usage of the birth number is prohibited by the Data Protection Law and a new unique identifier for information systems has not been introduced yet).

[14] Minerva is the methodology and the timetable of the implementation of eGovernment services provided on-line

Qualified certificate containing the unique identifier

Currently not in use.

There is no official authentication policy in Slovakia that defines a strict hierarchy of the different authentication systems in use.

Regional/local applications are not currently available, but if they will be in the future, their authentication resources will be different from application to application. A real example of a local application is the usage of university student cards. Since October 2004, each student at Slovakian universities is issued a student card in the form of a chip card (standard MIFARE MF1 IC S70). The electronic card contents the personal data of the student and identifies them if needed. Student cards are mainly used for library borrowing services, access control, and public transportation.

3.3.2 Legal framework

There is currently no legal framework in force related to the electronic identification of a person.

The main legal framework for personal identification in general is laid down in:

- Act No. 253/1998 Coll. on the notification of citizen residency and on the population register of the Slovak Republic (*Zákon o hlásení pobytu ob•anov Slovenskej republiky a o registri obyvate•ov Slovenskej republiky*)
- Act No. 301/1999 Coll. on the birth number. Also English version available (*Zákon o rodnom •ísle*):
- Act No. 224/2006 Coll. on identity cards (Zákon *o ob•ianskych preukazoch*)
- Act No. 154/1994 Coll. on Register Offices (*Zákon o matrikách*)
- Act No. 215/2002 Coll. on electronic signature (*Zákon o elektronickom podpise*)
- Civil Code, Act No. 40/1964 Coll. (*Ob•iansky zákonník*)
- Act No. 275/2006 Coll. on information systems of public administration (*Zákon o informa•ných systémoch verejnej správy*)
- Act No. 428/2002 Coll. on personal data protection (*Zákon o ochrane osobných údajov*)
- Decree of National Security Authority No. 339/2004 Coll. on security of technical devices (*Vyhláška Národného bezpe•nostného úradu o bezpe•nosti technických prostriedkov*)

The main legal framework on legal person identification/registers is laid down in:

- Act No. 455/1995 Coll. on trade enterprise (*Zákon o živnostenskom podnikaní*)

- Commercial Code, Act No. 513/1991 Coll. (*Obchodný zákonník*)
- Act No. 530/2003 Col. on commercial register (*Zákon o obchodnom registri*)
- Act No. 83/1990 Coll. on association of citizens (*Zákon o združovaní ob•anov*)
- Act No. 253/1998 Coll. on the notification of citizen residency and on the population register of the Slovak Republic (*Zákon o hlásení pobytu ob•anov Slovenskej republiky a o registri obyvate•ov Slovenskej republiky*)

It should be noted though that Slovakia has no specific regulations with regard to the process of authentication in general. There is no general provision saying how to identify a person in eGovernment applications. The authentication systems are mostly created ad hoc and are dedicated to a specific user group (application specific), because no generally used eID cards or tokens are in place.

The legal framework distinguishes between signatures and authentication, but a general legal framework for authentication is missing[15]. The e-Signatures law (Act No. 215/2002 Coll. on electronic signature) faithfully transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such, because the certificate and qualified certificate does not contain any unique personal identifier (see the issue mentioned above: the birth number is legally protected by the Data Protection Law and not usable for information systems and there is no new personal number available yet based on a cryptographic algorithm usable for information systems as a unique identifier of certificate holders).

Any legal entity is represented by a natural person – statutory representative who is entitled to act in name of legal entity. Statutory representative(s) is/are registered in the Commercial Register. If the legal entity has two or more statutory representatives, they can entitle one of them to act in name of the entity (e.g. in the area of electronic signatures the entitled statutory representative can be the holder of a qualified certificate and the company name can be given in a subject field as a pseudonym). But because of a lack of a general provision for authentication also the regulation for legal entities is missing.

The unique identifier (currently only the birth number) is legally protected by Data Protection Law[16]. Personal data may only be processed upon consent of the data subject, and Art. 8 (2) of the Data Protection Law further states that in the processing of personal data, the birth number may be used for the purposes of identification of a natural person only if its use is necessary for achieving the given purpose of the processing. The processing of a different identifier revealing characteristics of the data subject, or releasing of an identifier of general application shall be prohibited.

The Population register (included among others the birth number of natural persons) is not accessible for private companies and also not for public administrative bodies. Only special categories of bodies (the Slovak Information Service – SIS, Police and National Security Authority) have an access to it and are able to browse the Population Register and to use data from it.

[15] Only in the secondary legislation (Decree of National Security Authority No. 339/2004 Coll. on security of technical devices) defines the notion authentication of a user as a confirmation of user identity according to authentication level based on comparison of an access user identifier with a value saved in access resource.

[16] Act No. 428/2002 Coll. on personal data protection.

3.3.3 Technical aspects

Because there is no real and standardized eIDM system in Slovakia, all questions with regard to technical aspects cannot be answered.

With regard to future plans, when there will be a central eIDM system, the authentication mechanism will be based on PKI and the private key will be included on the smart card with contact ICs (specified in ISO 7816) or with dual interface ICs (one chip and two interfaces – contact ISO 7816 and contact-less ISO 14443). At this point, only the political strategy has been adopted (initiative mentioned above – from Action Plan Minerva), but no decision about technical solutions has been made yet.

3.3.4 Organisational aspects

As was already mentioned several times Slovakia has no centralised eIDM system usable for all eGovernment application. Because the functionality of all eGovernment applications varies from application to application also electronic identity management is different and it is very hard to describe some general characteristics.

eGovernment applications including eIDM systems are managed by public administration bodies (ministries or central public administration bodies) that maintain the information. Responsibility for the actuality of information included in the eIDM system and for the potential errors is appointed to the administrator of the information system, who is responsible for processing personal data received through registration according to Data Protection Law.

With regard to authorisation management, there is no generic policy or infrastructure in place yet. A few ad hoc solutions exist, that use the 3 kinds of authentication/identification mentioned above:

Basic user name and password

In general this kind of eIDM system is introduced in the eTendering application managed by the Public Procurement Office. Currently the system is openly accessible to anyone, and merely requires on-line registration. After the registration the system is accessible to anyone, also for non-nationals. After the registration, the user receives his software certificate and password via e-mail. After this registration process the user can communicate with a public body using the requested identifier/password and software certificate.

Qualified certificates and prior personal identification

The primary requirement is to have a valid qualified certificate. If the qualified certificate does not contain a unique identifier (which is currently typically the case because there is no unique identifier in place), its holder is not sufficiently identified for communication with public administrations. That is the reason why the user first has to come in person to the public administration body which provides the system/application, in order to verify the personal data of the certificate holder. During this registration process, the identity of a user is proven by using conventional identity cards which is matched with the serial number of qualified certificate. This is the way in which the eTax system, eServices of Commercial Register and several other eGovernment applications operate.

Qualified certificate with unique identifier

When using this method of authentication, the person has to fill in a form containing his personal data which he/she then signs by qualified electronic signature. Its private key is stored in a secure signature creation device. The provider of an eIDM system verifies if the data in the form corresponds to the data in a qualified certificate issued by an accredited CSP (this can be done automatically or manually). If the person fills the form with incorrect identification data, this is considered an attempt to fraud and the person is responsible for it.

3.4 Interoperability

Almost all eGovernment applications/systems are accessible to qualified certificate holders, who have been identified by public administration bodies. In practice, those systems are accessible only to holders of a qualified certificate from CSPs accredited in the Slovak Republic (currently there is also one Czech CSP accredited in Slovakia, so that the qualified certificates from this CSP are also recognised).

Slovakia has no agreements with other governments ensuring users access using their own authentication method. There are also no strategies and plans to improve eIDM means for non-nationals.

3.5 eIDM Applications

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

Basic user name and password

In general this kind of eIDM system is used in the eTendering application[17] https://evo.gov.sk managed by the Public Procurement Office (see also above). Currently the system is openly accessible to anyone, and merely requires on-line registration.

Qualified certificates and prior personal identification

This system (see also above) is used in the eTax system[18] http://drsr.sk, the eServices of Commercial Register[19] http://www.orsr.sk and several other eGovernment applications.

3.6 Future trends/expectations

There is a plan to introduce a Slovakian eID Card with a chip card and qualified electronic signature at the end of the next year according to the task No. 10 of the Action Plan Minerva. Before this can be done, it is necessary to introduce a new unique identifier for the communication between information systems of public administration. These are two main tasks for the following years.

Until this is done, it will not be possible in a electronic way to identify an entity and a few paper based steps will continue to be further required (prior registration via traditional identity card etc.).

[17] The real operation planed for 1 January 2007 postponed, no usage statistic available.

[18] In a year 2005 only 936 tax declarations were filed electronically (approximately 50 signed by qualified electronic signature).

[19] The real operation will start from 1 August 2007, no actual usage statistic available.

3.7 Assessment

The Slovakian approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.7.1 Advantages:

- Freedom in implementation of any authentication solution (lack of legal framework , where is laid down how it is possible to authenticate user)

3.7.2 Disadvantages:

- Differences between eIDM system cause that those systems are not interoperable (different authentication means for every application)
- Very low number of potential users, because they have to do a lot of steps to use one system
- Lack of legal framework for authentication, that causes the disadvantages and issues mentioned here
- Lack of eID cards