IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE SLOVENIA

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 Slovenian 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

eGovernment applications use eIDM systems based on qualified certificates from registered certification authorities (CSPs) comprising one governmental CPS and private sector CSPs issuing certificates (either software certificates or smart card based). Currently, the following CSPs are registered in Slovenia:

1. Certification authority at the Ministry of Public Administration (in Slovene "*Overitelj na Ministrstvu za javno upravo*"), Tržaška cest 21, SI-1000 Ljubljana, Web: http://www.ca.gov.si.
2. HALCOM informatika d.o.o., HALCOM informatika d.o.o., Tržaška cesta 118, SI-1000 Ljubljana, Web: http://www.halcom.si
3. AC NLB (Certification Authority at the bank "*Nova ljubljanska banka*"), Šmartinska 132, SI-1520 Ljubljana, Web: http://www.nlb.si/acnlb.
4. POŠTA®CA (Pošta Slovenije), Slomškov trg 10, SI-2500 Maribor Web: http://postarca.posta.si.

CSPs in Slovenia use different approaches in mapping a single certificate to its holder's identification data (e.g. tax number or Personal Registration Number) but all of them manage some connection between the user and his certificate. Some Certification Authorities simply add the tax ID number in certificates, while others add unique certificate identification (a certificate serial number) to a certificate and keep all the data in a stand-alone database (like the Certification authority at the Ministry of Public Administration).

Alternative eIDM systems are the Slovenian Health Insurance Card System (in Slovene "*Zavod za zdravstveno zavarovanje Slovenije*, Slovenian abbreviation: ZZZS) that has been introduced in the years 1999/2000 by the Health Insurance Institute of Slovenia (HIIS) following the European Union recommendations for a health card system. Within this system two types of electronic identification cards are used:

- Health Insurance Card (HIC) and
- Health Professional Card (HPC).

The first one is issued to every insured person in Slovenia; the latter one is used to identify health care professionals. These cards are used to identify insured persons and health professionals within the health care system and health insurance system of Slovenia. At present they cannot be used for identification/authentication in eGovernment applications.

A Slovenian national eID project (in the sense of a modernisation of conventional ID cards) officially started in February 2003 by establishing a project group; however the project was suspended. It is expected that the project will roll-out again in 2008.

In Slovenia every citizen has:

- Personal Registration Number;
- Tax Number; and
- Health Insurance Number

Every legal person has:

- Identification Number and
- VAT Number.

Identification information with regard to natural persons: Every Slovenian citizen becomes registered in the Slovenian Central Register of Population (CRP) and receives a unique Personal Registration Number (PRN; Slovenian abbreviation: EMŠO) as defined in the Central Population Register Act. Other individuals, who have no PRN but have to exercise rights or duties in Slovenia, also become registered with the CRP.

Health insurance identification for natural person: the identifier is the "unique identification insurance number" (HIIS number, in Slovene "*številka ZZZS*"). Every Slovenian citizen receives this number which is managed by Health Insurance Institute of Slovenia.

Identification information with regard to legal persons: The Business Register of Slovenia contains records of all legal entities registered, recorded or created by law, irrespective of their business activity, Commercial Register of Slovenia Act. Every entity holds a uniform 7-digit identification number.

The tax number (TIN) in Slovenia is defined by the Tax Administration Act. It was introduced as a unique register of identification data of all taxpayers, as an official source of registration data and as the system for exchange of information with other state registers. The tax number is the identification sign which defines the taxpayer (individuals and legal entities), and it is used for uniform specification and connection of data in tax records about the taxpayer, which are managed by the Tax Administration. The tax number is used for all taxes. When Slovenia joined the EU, the TIN got the prefix SI (code for Slovenia) for VAT purposes.

All of these systems will be discussed in greater detail below.

From a practical perspective, usage and uptake can be summarised as follows:

eIDM system	Potential user base	Actual penetration	Actual use
Certification authority at the Ministry of Public Administration	2 million (entire population) - for natural persons 100.000 organizations with approx. 915.000 employees	approx. 40.000 certificates	approx. 75%

	(all registered business entities in Slovenia) – for business entities approx. 45.000 (all public employees)	7.600 organizations with approx. 20.000 certificates approx. 8.500 certificates	approx. 75% approx. 75%
Halcom-CA	2 million (entire population) - for natural persons 100.000 organizations with approx. 915.000 employees (all registered business entities in Slovenia) – for business entities	No public statistics are available	No public statistics are available
AC NLB	Public statistics are available for 2005: approx. 600.000 bank account holders	Public statistics are available for 2005: approx. 90.000 users of e-banking	No public statistics are available
POŠTA®CA	2 million (entire population) - for natural persons 100.000 organizations with approx. 915.000 employees (all registered business entities in Slovenia) – for business entities	No public statistics are available	No public statistics are available
Health cards	2 million (entire population) - Health insurance cards 23.000 (all health professionals) - Health professional cards	2 million 20.600	2 million 18.000

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The use of eIDM systems in the context of eGovernment in Slovenia until 2010 is coordinated reasonably well. Steps are being taken towards the provisions needed for the development for central information and telecommunications infrastructure for eGovernment including the usage of horizontal integration for authentication processes based on certificates and their implementation or username/passwords (One-Stop-Shop concept). The use of this infrastructure will enable to achieve lower costs of development and operation of eGovernment, increased quality and uniformity of solutions and interoperability.

One of the purposes of horizontal integration is to share information so as to avoid requesting it twice from citizens or companies. This is the so-called “authentic source” principle: once information has been requested from the user, it should be stored in a single authentic source. All other eGovernment services are then expected to access the information through the authentic source whenever possible, rather than requesting it multiple times.

EGovernment is driven by the following services:

- *National eGovernment*

  eGovernment Strategy of the Republic of Slovenia for the period 2006 to 2010 (abb.: SEP-2010): SEP-2010 was issued at the beginning of 2006. The purpose of the strategy is to determine the framework and goals for the further realisation of new and already established eGovernment activities, with emphasis on user satisfaction, rationalisation of administrative operations and modern electronic services, which will enable a higher quality of life and give the administration a more friendly face during contacts with users.

  One of the provisions needed for the development of eGovernment until 2010 is also a central information and telecommunications infrastructure for eGovernment. The use of this infrastructure will enable to achieve lower costs of development and operation of eGovernment, increased quality and uniformity of solutions and interoperability. Among others, this also includes the usage of authentication processes based on qualified certificates and their implementation or username/passwords, drawing up of security policies, consistent implementation of security policies and taking into account legislation in this field (e.g. protection of personal data, information of public character). SEP 2010 is available at:

  http://www.mju.gov.si/en/legislation/important_documents/

- *Local eGovernment*

The strategy for local self-government has its basis in the eGovernment Strategy for Local Self-Government (abbr.: ESLS), prepared in 2003. The reason for introducing the different strategy lies in the fact that municipalities had different levels of informatization, which depended upon the size of each municipality and related resources. Consequently common solutions and roadmaps were needed, which were prepared within the strategy. In addition the goal of the strategy was also to connect central government with local government in the field of e-services. Due to their complexity, importance and size, the joint or basic projects discussed in the strategy will be a part of the eGovernment projects which will result from SEP-2010. The state administration will provide a central information and telecommunications infrastructure for eGovernment (see Section 9 in SEP-2010) with agreed conditions of use also for eIDM systems based on digital certificates based applications.

Based on the ESLS and SEP-2010 the corresponding Action Plan for local self-government is currently in preparation.

ESLS is available in Slovene only at

http://www.svlr.gov.si/si/delovna_podrocja/podrocje_lokalne_samouprave/informatizacija_obcin/.

- *eHealth 2010 strategy:*

In December 2005, the Ministry of Health of Slovenia launched its Information Technology Implementation Strategy for the Health Care System of Slovenia: *e*-Health^{2010} (in Slovene "*e-Zdravje*^{2010}").

The strategy in its introduction describes IT achievements in the Slovene health care system, EU expectations, visions and initial tasks. The strategy highlights three strategic components:

- the building of the national health care ICT infrastructure,
- single Health Care information portal and
- introduction of the Electronic Health Record.

The vision for 2010 is to establish:

- efficient, flexible informatics to support strategic goals of national health-care (HC) system to serve the needs and best interests of the citizens, HC professionals, HC organisation management, HC service purchasers and HC system administrators,
- interlinking of information system islands to facilitate the access to information and direct communication across the administrative and organisational barriers to both the citizen and to the HC professional.

At the beginning, three national bodies were established: the Council for Health Care Informatics, the Committee for Standards in Health Informatics, both to be supported by the Project Unit for Health Informatics.

e-Health2010 is accessible on:

http://www.mz.gov.si/fileadmin/mz.gov.si/pageuploads/mz_dokumenti/delovna_podrocja/zdravstveno_varstvo/kodele/ezdravje_ang.pdf

- *Information Society:*

Information Society Strategy until year 2010 (abb.: SI2010): this strategy is currently in finalization. SI2010 will follow the i2010 - COM(2005) 229 and will comprise of the major components of already available national strategies in the ICT field, such as eGovernment strategy, eHealth strategy, etc.

The draft version is available in Slovenian only at (it is expected to be adopted by the Government of Slovenia in April 2007):

http://www.mvzt.gov.si/si/novinarsko_sredisce/novica/article/94/5369/?cHash=ee405eefc0

3.2.2 National eGovernment cooperation and coordination

- *At the national level:*

According to the agreed organisation with respect to eGovernment projects there are the following designated bodies:

- The highest decision-making authority for eGovernment projects is the Co-ordinating Body for Better Public Administration.
- For harmonisation of the management of this area a working group for eGovernment project co-ordination has been established, which is made up of members appointed from ministries, their component authorities and government offices, which are in charge of e-services and/or e-services infrastructure in the eGovernment Action Plan.

As the public institution the Ministry of Public Administration, established in December 2004, is responsible for the development, implementation and co-ordination of eGovernment in Slovenia. In particular the e-Government Development Section within the Ministry's Directorate for e-Government and Administrative Processes supports the development of the e-government strategy, and prepares and monitors the implementation of the strategy and action plan. The Directorate for e-Government and Administrative Processes is in charge of developing the country's e-government infrastructure at an operational level, and to support, control and coordinate departmental ICT projects. Major tasks will also be performed by all public administration authorities (state authorities, local self-government) who will assist in the opening of key administrative registers and revising procedures for more efficient work in administration (http://www.mju.gov.si/?L=1).

As stated in SEP-2010, the national interoperability framework is needed to attain the planned development of eGovernment until 2010. SEP-2010 defines the interoperability framework as linking of all elements (standards and recommendations, uniform architecture, open standards and solutions, guidelines) in a national interoperability framework for eGovernment services and solutions, which will provide organisational, semantic and technical interoperability and, at the same time, creative co-operation when it comes to the preparation of an interoperability framework for pan-European services.

With this in mind the development of the national interoperability framework has just started along with the broad program dedicated to electronic connection and interchange of data between the national registers. The two programs will be developed in parallel since they are to share common results and solutions.

- *At the local level:*

The major responsibility for local government is in the hands of the Government Office for Local Self Government and Regional Policy. Their recommendations and guidelines are published on the following web site: (http://www.svlr.gov.si/si/delovna_podrocja/podrocje_lokalne_samouprave/informatizacija_obcin/) which comprises of a strategy and action plan, list of projects for local government with XML schemas, the system of e-forms, guidelines for access to registers, common documents, etc., which may be considered as parts of the future interoperability framework.

- *eHealth:*

National coordination is performed by the following bodies:

- National Council for HC Informatics (in Slovene "*Svet za informatiko v zdravstvu –SIZ*", http://www.mz.gov.si/si/informatika_v_zdravstvu_siz_ozis/svet_za_informatiko_v_zdravstvu_siz/);
- HC Informatics Standardisation Board (in Slovene "*Odbor za zdravstveno informacijske standarde - OZIS*", http://www.mz.gov.si/si/informatika_v_zdravstvu_siz_ozis/odbor_za_zdravstveno_informacijske_standarde_ozis/);
- HC Informatics Centre;
- (Interdepartmental) HC Informatics Strategic Board for the development of health care

The National Council for HC Informatics established within the Ministry of Health carries out the following tasks:

- development of the strategy for an integrated health care informatics system;
- co-ordination of the development of new projects and continue with those already in place;
- planning and co-ordination the introduction of common information and communication infrastructure;
- co-ordination the formation and adoption of standards;
- determination the criteria and standards for safeguarding and ensuring quality of information in health care information systems;

- planning and co-ordination pilot projects;
- monitoring, promotion and dissemination of best practices;
- forming the standards of e-Health for health service providers and to ensure the realisation of the strategy.

3.2.3 Traditional identity resources

Identity card

The identity card is defined in the Identity Card Act (Official Gazette of the RS, No. 75/1997, 60/2005) and isn't obligatory in Slovenia. However, every adult person must posses a valid official identification document with the photo (identity card, passport, or driving license). Every Slovene citizen with permanent residence in Slovenia is entitled to posses an identity card, which can be issued also to an underage person if his/her parents or legal representative apply for it. Besides, a Slovene citizen with temporary residence in Slovenia can obtain an identity card if he/she is 18 years old and doesn't posses a valid official identification document. The identity card is issued for a period of validity of 10 years for adults and 5 years for the underage. An application form for an identity card can be filed in every administrative unit (there are 58 such offices in Slovenia) or information office. Total cost of identity card is approximately 16.50 EUR for an adult person. The identity card can be also used as a travel document in EU Member States, Croatia, Iceland, Liechtenstein, Norway and Switzerland.

An identity card for non-nationals is issued by the administrative unit to a non-national with a permanent residence permit in the Republic of Slovenia, who has reached the age of 18 years. Non-nationals must apply for an identity card within 30 days of being granted a permanent residence permit. The identity card is issued also to non-nationals with a temporary residence permit if they apply for it. The identity card for non-nationals with a permanent residence permit is issued for a period of validity of 10 years whereas the identity card for non-nationals with a temporary residence permit is issued for the period of validity equal to that of the temporary residence permit. The identity card for non-nationals may be issued also to persons with a permanent or temporary residence who have reached the age of 15 years, if they submit such a request in which case the identity card is issued for a period of validity not exceeding five years.

Identification numbers

In Slovenia every citizen has:

- Personal Registration Number,
- Tax Number and
- Health Insurance Number.

Every legal person has:

- Identification Number and

- VAT Number.

Personal registration number

Every Slovenian citizen becomes registered the Slovenian Central Register of Population (CRP) and receives a unique Personal Registration Number (PRN; Slovenian abbreviation: EMŠO) defined in Central Population Register Act (Official Gazette of the RS, No. 1/1999, 54/2002, 39/2006). Other individuals, who have no PRN but have to exercise rights or duties in Slovenia, also become registered with the CRP.

Persons can be entered into the CRP in few distinct ways, but the most common possibilities include registration at birth and naturalization. During registration every person receives a PRN which is a thirteen-digit number based on date of birth and gender with the following meaning:

- the first seven digits represent date of birth in format DDMMYYY,
- the next two digits represent label of the register (50),
- the following three digits are a combination of gender and consecutive number for persons born on the same date (000-499 for men and 500-999 for women),

the thirteenth digit is a control number, calculated according to module 11.

The CRP is primarily used to centrally collect, manage, store and use data on Slovene inhabitants with the main purpose to control status and fluctuation of population. It is used by state institutions and other users that need the information included in the register in order to perform their duties, manage their own databases and carry out statistical, socioeconomic and other researches. Because of the nature of the data kept in the CRP all its users are required to have proper legal basis. The CRP is managed by the Ministry of Interior.

The CRP is the central database on:

- Slovene citizens with temporary or permanent residence in Slovenia and non-nationals mandated to temporarily or permanently reside in Slovenia;
- Slovene citizens that live abroad permanently or longer than 3 months;
- non-nationals without mandate to reside in Slovenia but who have certain rights or obligations (i.e. pension or social insurance, taxes, humanitarian reasons).

For each person the CRP contains following information: PRN, place of birth, name and surname, citizenship, type and address of residence, marital status, formal education, voting rights, mother's PRN, father's PRN, spouse's PRN, PRNs of children, identifiers for interconnection to other administrative databases, dates and data of events, changes or corrections.

Since the CRP is a central database and contains quite distinct information it is necessary that data is acquired from other registers. In principle all the data are collected from the primary registers such as birth/death register, court register, tax register, spatial register, educational registers etc. Institutions that manage those registers are obliged to provide all relevant information in a certain format, on time and free of charge. Because the CRP is a register with great importance all the data are kept for 100 years after person's death or emigration; and after that they are moved to the Archive of the Republic of Slovenia.

Identification number for legal persons

The Business Register of Slovenia contains records of all business entities registered, recorded or created by law, irrespective of their business activity. The Commercial Register of Slovenia Act (Official Gazette of the RS, No. 49/2006) regulates managing of the Business Register, defines business entities and their identification numbers, the content of the register, the process of entity registration and proper usages of data stored in the register. Every entity holds a uniform 7-digit Identification Number that is assigned to the entity when it gets registered in the primary register. When the entity is deleted from the Business Register its Identification Number remains valid and must not be reused. Identification Number is intended to be used in data exchange between business entities themselves and registration offices.

Registration of the entity in the Business Register can be performed in different ways: business entities whose primary register is the Business Register (i.e. entrepreneurs) are automatically entered during their initial registration, business entities that are established based on the legislation and not registered elsewhere must submit registration forms, all other business entities are entered into the Business Register after their registration at the proper registration office.

The contents of the Business Register vary depending on the type of the business entity and may contain following data: registration date in the Business Registry, Identification Number, TIN and identification of VAT registration, name, short name, postal address, foundation date, data on registration (registration office, date, registration number), registered business activities, main business activity, institutional domain, type of business entity, type of society, special status, budget identifier, business entity size according to the Slovene legislation and to EU standards, data on founders (name, address, EMŠO or Identification Number, TIN), type of foundation funds, countries of foundation funds, type of ownership, percentage of state ownership, data on ownerships in other business entities, data on authorized persons (name, address, TIN, EMŠO, type), identification of activity, numbers of bank accounts, identifier of obligation to publish public information, data on business termination initialization, other contact information (phone and fax numbers, e-mail and internet address), data on changes (type and date), data on entity deletion (type, date and legal successor).

The Business Register contains very distinct data and therefore they are derived from a number of other registers and institutions (the CRP, the tax register, the Court Register, the Central Bank of Slovenia, the Ministry of Finance, the Ministry of Public Administration, etc.). All digital data of the registry is kept permanently whereas paper documentation is preserved for two years only. The register is managed by the Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES). Public data of the Business Register are available to the public free of charge and AJPES publishes them on its web page. Besides current data of all business entities the register also contains information of every registration, change and deletion of entities. From June 2007 the Business Register will be expanded with the list of digital certificates of authorized persons for every business entity from the register. When established it will be publicly available on the internet as a web page and a web service and it will enable users to check whether a single certificate belongs to an authorized person of an appointed business entity. The list will contain the following information:

identifier of the business entity (Identification Number, TIN), identifier of the certificate (CA identifier, serial number), identifier of the authorized person (TIN).

Tax numbers

The tax number (TIN) in Slovenia is defined by the Tax Administration Act (Official Gazette of the RS, No. 17/05, 59/05). It was introduced in 1996 as a unique register of identification data of all taxpayers, as the official source of registration data and as the system for exchange of information with other state registers. The tax number is the identification sign which defines the taxpayer (individuals and legal entities) and which is used for the uniform specification and connection of data in tax records about the taxpayer, which are managed by the Tax Administration. The tax number is used for all taxes. When Slovenia joined the EU, the TIN got the prefix SI (code for Slovenia) for VAT purposes. The tax number is a random eight-digit number (first digit cannot be 0):

- the first seven digits represent the basic number, which is a randomly chosen number from number range from 1,000,000 to 9,999,999.
- the eighth digit is a control number, calculated according to module 11.

All individuals with permanent or temporary residence in the Republic of Slovenia and persons, obliged by law to submit the application for entry into the tax register to the Tax Administration but who fail to meet this obligation, are entered into the tax register out of official duty. Natural persons who are independently professionally active (i.e. as entrepreneurs) and legal persons are entered into the tax register out of official duty, too. The Tax Administration acquires data for the entry of persons out of official duty from official registers and records. For individuals most of data is acquired from the CRP whereas the Business Register represents a main source for data on entrepreneurs. It is also used for acquiring data on legal persons but the primary register for them is the Court Register. All other entities are entered into the tax register on the basis of application for entry into the tax register.

For every individual the tax register contains the following information: TIN, identification of VAT registration, personal data (name and surname, gender, place and date of birth, date of death, PRN), citizenship, residential status, address of permanent and temporary residence, numbers of bank accounts, employment status (unemployed / employee / pensioner / farmer / student / pupil, employer's data), family data (spouse's name, address and TIN, names, addresses and TINs of children), data on authorized persons (TIN, name, address, type, limits and validity of authorization, data on his/her digital certificate), data on person's digital certificate, capital investments in Slovenia and abroad, reason of registration (permanent or temporary residence, amount of property, professional activity…).

On the other hand the tax register contains the following information of legal persons: TIN, identification of VAT registration, name and address (postal address, phone and fax numbers, e-mail address), foundation data (date of beginning and ending, registration office, registration number), type of legal person, amount of basic funds, tax period, residential status, number and locations of business places, data on branch offices in Slovenia and abroad, data on founders/members (TIN, name, address, type and limits of responsibilities, date of validity, amount), capital investments in Slovenia and abroad, data on authorized persons (TIN, name, address, type, limits and validity of authorization, data on his/her digital certificate), Identification Number, identifiers of business activities, numbers of bank accounts, TINs and numbers of bank accounts for connected persons, accountant's data (TIN, name, address), data on business termination (date of first and final decision, type of decision), data on changes of status.

Health insurance number

Health insurance identification for natural person: the identifier is the "unique identification insurance number" (HIIS number, in Slovene "*številka ZZZS*"). Every Slovenian citizen receives this number managed by the Health Insurance Institute of Slovenia. The HIIS number is unique and cannot be derived form other identifiers, e.g. from PRN. The HIIS number is a successive nine-digit number (entering the insurance), starting from 02000000x. The ninth digit is a control number.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Main eID systems based on qualified certificates

There are four Certificate Service Providers (CSPs) delivering certificates to the public in Slovenia that are registered at the Ministry of Higher Education, Science and Technology. All of them issue qualified certificate, although the legislation requires registration of any CSP issuing certificates to the public. The reason for this situation is probably that it is relatively easy for a CSP to fulfil the technical requirements for issuing qualified certificates, and by issuing these a CSP puts himself in the same position as other CSPs have. Currently the following CSPs are registered in Slovenia:

1. Certification authority at the Ministry of Public Administration (in Slovene "*Overitelj na Ministrstvu za javno upravo*"), Web: http://www.ca.gov.si.
2. HALCOM informatika d.o.o., Tržaška cesta 118, SI-1000 Ljubljana, Web: http://www.halcom.si
3. AC NLB (Certification Authority at the bank "*Nova ljubljanska banka*"), Šmartinska 132, SI-1520 Ljubljana, Web: http://www.nlb.si/acnlb.
4. POŠTA®CA (Pošta Slovenije), Slomškov trg 10, SI-2500 Maribor Web: http://postarca.posta.si.

Data relating to the Certificate Service Providers from the register are accessible at web site http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/REGISTER_OVERITELJEV_V_RS_ver16__03.04.2006.pdf (in Slovenian only).

It is worth mentioning that the registration of CSPs is quite an easy and fluent procedure which takes place since the adoption of ECESA act. All the changed data about a CSP (i.e. additional services) are regularly published in the registry. On the other hand, the possibility of installing a voluntary accreditation scheme hasn't been brought into force yet – at the moment there is no accreditation office determined. Probably CSPs didn't find any advantages that could be gained as an accredited CSP.

All above mentioned CSPs began issuing digital certificates with clear intentions and expectations about their users. The CSP at the Ministry of Public Administration started issuing certificates to the public to promote e-government applications, CSPs HALCOM-CA and AC NLB focused primarily on issuing certificates for e-banking, while CSP POŠTA®CA started issuing digital certificates as a part of a service called »Secure mailbox« which is also offered by the Slovene Post. In spite of the above mentioned basic purposes of issuing digital certificates more and more independent e-service providers arose that offered applications or services based on digital certificates, and since they didn't issue their own certificates they often relied on established CSPs and certificates that were issued by them. E-service providers take different approaches in selecting supported CSPs – some rely only on certificates issued by a specific CSP, others define groups of CSPs – but the most frequent solution is to support all qualified digital certificates issued by registered CSPs. We can establish that this became almost a »de facto« standard in e-services in Slovenia and e-government applications follow it by putting this demand into the Decree on administrative operations.

The e-government applications for citizens and private sector can be performed by any qualified certificates issued by registered CSPs, given above. All of them are based on prior physical identification, i.e. the requesting party needs to appear personally before the CA to receive his credentials. As trusted third parties they can deliver PKI based digital certificates for the generation of secure electronic signatures in eGovernment applications. Such certificates are widely used in different eGovernment applications.

Connection and interchange of data between national registers

Certification Authorities in Slovenia use different approaches in mapping single certificates with its holder's identification data (e.g. tax number or Personal Registration Number) but all of them manage some connection between the user and his certificate. Some Certification Authorities simply add the tax ID number in certificates, while others add a unique certificate identification (serial number) to a certificate and keep all the data in a stand-alone database (like the Certification authority at the Ministry of Public Administration). Personal data in this database can only be used under conditions regulated in Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/2004, 113/2005-ZInfP). Usually there are two levels of personal data usage available depending on legal bases for data providing:

- personal data checking,
- personal data acquiring.

Certification Authorities keep different kinds of user data:

- Personal Registration Number and/or Tax Number for citizen,
- Identification Number and/or VAT number for legal person.

Certification Authorities that keep data in stand-alone database offer different interfaces for applications to connect to the database; usually there is a web-service (SOAP) or some other kind of interface (ODBC, JDBC) available.

Details on mapping between the certificate and its holder for all Certification Authorities in Slovenia are given below.

The health insurance card

The health insurance card is a document applied in the implementation of rights deriving from compulsory and voluntary health insurance in Slovenia. It is issued free of charge, to every person upon the first establishment of the compulsory health insurance status in Slovenia. The card data are updated by the card holder autonomously, through the self-service terminals installed throughout the national territory.

The data, recorded electronically in the card chip, are protected against unauthorised access by being accessible only to the holders of health professional cards. This ensures a high security level, the significance of which is growing along with the progressive extension of the card data set.

The card provides easy, fast and accurate transmission of data between the insured persons, health insurance providers and health care service providers. This arrangement simplifies a number of procedures, and, in particular, is friendly to the insured persons, as it eases administrative barriers in their implementation of health insurance rights.

The card system is aligned with the needs of the Slovene health care and health insurance, while also complying with the international recommendations and standards. It is worth emphasising that Slovenia was the first country to introduce an electronic card at a national scale, and that other EU member countries are introducing similar infrastructure. The common objective of the EU member countries is to introduce an electronic document applicable both within a country and across its borders.

The card holds electronic records of the following data items:

- card holder (name and surname, address, sex, date of birth);
- health insurance contribution obligor (registration number, title, address, type of contribution obligor);
- compulsory health insurance (validity data);
- voluntary health insurance (Insurance provider, type of policy, validity data);
- selected personal physician (general physician/paediatrician, dentist, gynaecologist);
- issued medical technical aids;
- voluntary commitment to posthumously donate organs and tissues for transplants;
- issued medication.

Authentication policies

There is no official authentication policy in Slovenia that defines a strict hierarchy of the different authentication systems in use. However, with regard to natural persons, there are four levels of authentication above public access:

- no authentication for public information and services
- on line by entering the personal data to register (user chooses his password and username) identity and then for authentication by assigned user number in combination with a password chosen by the user

- basic username/password (after registration using official register numbers),
- use of qualified certificates for signature and authentication.

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering personal data	By personal data entered on line	Information/services of limited sensitivity
2	Level 1 + send-out of a confirmation e-mail with username, initial password and activation URL to an address indicated by the citizen	By assigned combination of a username and password chosen by the user	Information/services of medium sensitivity
3	Physical identification at the registration authority for the acquisition of qualified certificate	Authentication/signature certificate + password	Information/services of high sensitivity and services requiring an electronic signature

3.3.2 Legal framework

The main legal framework for the eID systems is laid down in:

- Electronic Commerce and Electronic Signature Act of 13 June 2000, coming into force on 22 August 2000. It provides the legal basis for using e-signatures and developing e-services in Slovenia (Official Gazette of the RS, No. 57/2000, 25/04),
- the Decree on Conditions for Electronic Commerce and Electronic Signing (Official Gazette of the Republic of Slovenia, No. 77/2000 and 2/2001)
- Rules on official registration procedure for certification authorities register of the Republic of Slovenia (Official Gazette of the RS, No. 99-4859/2001)
- Access to Public Information Act (Official Gazette of the RS, No. 51/2006), law on access to information and documents produced by public institutions;
- Personal Data Protection Act (Official Gazette of the RS, No. 86/2004, 113/2005-ZInfP), regulating rights, obligations, principles and measurements to prevent illegal encroachment upon someone's rights with regards to her/his personal data. The databases of the certificates and personal data of their holder are regulated by this act;
- The Central Population Register Act (Official Gazette of the RS, No. 1/1999, 54/2002, 39/2006): Law on central population register and personal number
- Tax Procedure Act (Official Gazette of the RS, No. 54/2004, 57/2004-ZDS-1, 109/2004 Odl.US: U-I-356/02-14, 128/2004 Odl.US: U-I-166/03-12, 139/2004, 56/2005 Skl.US: U-I-159/05-4, 96/2005-ZRTVS-1, 100/2005 Odl.US: U-I-159/05-14, 109/2005); Law on tax number and tax procedures

- Health Care and Health Insurance Act (Official Gazette of the RS, No. 72/2006) (http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO213.html);
- Healthcare Databases Act (Official Gazette of the RS, No. 65/2000), http://zakonodaja.gov.si/rpsi/r09/predpis_ZAKO1419.html; regulating the right of access to health documentation which relates to their state of health, except where the physician assesses that this would have a harmful influence on the patient's state of health
- Commercial Register of Slovenia Act (Official Gazette of the RS, No. 49/2006); Law on Commercial Register of Slovenia holding
- Access to Public Information Act (Official Gazette of the RS, No. 51/2006); Law on access to information and documents produced by public institutions

The question of authentication is not especially emphasized by law.

There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).

3.3.3 Technical aspects

Qualified certificates

As already mentioned almost all e-government applications for citizens and private sector as well as lots of private sector applications can be accessed by qualified certificates issued by any registered CSPs. In practise this means that qualified digital certificates represent the dominant eIDM token used in Slovenia. It is estimated that this situation will not change until the eID card is introduced. In the following paragraphs basic facts about all four registered CSP's and certificates that they issue are presented.

Certification authority at the Ministry of Public Administration

There are two distinct issuers of digital certificates at this CA: SIGOV-CA and SIGEN-CA. SIGOV-CA issues digital certificates to public servants. On the other hand SIGEN-CA issues certificates to natural and legal persons. Non-nationals and foreign entities can obtain digital certificates from SIGOV-CA if they are employed in a public institution and from SIGEN-CA if they are residents of Slovenia. In order to get a certificate, the user must fill out an application form and file it at the registration authority. Registration Authorities for SIGOV-CA are established at several institutions while Registration Authorities for SIGEN-CA can be found:

- at the administrative units in Slovenia and consulates for natural persons,
- at the tax offices in Slovenia for legal persons.

There are different types of users that can obtain certificates:

- SIGOV-CA: governmental employees, organizational units of institutions and servers,
- SIGEN-CA: citizens, employees, organizational units of companies and servers.

CA issues following types of certificates:

- web certificate has single key pair and is mostly used in web browsers; it can be used for creating digital signatures and encrypting data; these certificates are most frequently used in web applications and S/MIME communication between users,
- advanced certificates consists of two key pairs: one for digital signing and the other for encrypting data; in order to use this certificate a special application (middleware) is needed; these certificates are mainly used in dedicated applications but can be also used in browsers and S/MIME clients.

All certificates issued by SIGOV-CA (except for servers) are kept on smartcards so that every certificate holder is equipped with an ActivCard smartcard and COM, USB or PCMCIA reader. Certificates issued by SIGEN-CA can be stored on a smartcard but can be also used as a software certificates. CA uses CRLs as a certificate validation system and publishes them on-line.

Every certificate contains a unique identification (serial number) that is created and added by a Certification Authority to the distinct name of the certificate and to the certificate itself. This serial number is used to map the certificate to its holder when certificate is used in different applications.

An example of a distinct name for a legal person's certificate is as follows:

```
c=si, o=state-institutions, ou=sigen-ca, ou=companies, ou=GZS – 73354376,
            cn=Ivan Cankar + serialNumber=2345752320017,
```

where "GZS" stands for short name of the company name, "73354376" stands for its VAT number, a person named "Ivan Cankar" is a company employee and certificate holder, and serial number "2345752320017" is created by SIGEN-CA following special rules.

All certificates' serial numbers created by SIGEN-CA and SIGOV-CA are kept in a stand-alone database, so called *Connectional table*, holding the serial number of the digital certificate, the holder's ID number (Personal Registration Number), the holder's tax number, the Identification Number of a legal person and the VAT number of a legal person.

Personal data in this database can only be used under conditions regulated in Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/2004, 113/2005-ZInfP). There are two levels of personal data usage available depending on legal bases for data providing:

- personal data checking,
- personal data acquiring.

HALCOM-CA

HALCOM-CA issues qualified digital certificates to natural and legal persons. Non-nationals and foreign entities can obtain digital certificates if they are residents of Slovenia. Natural persons can apply for certificate electronically but physical identification at Registration Authority is needed. Registration Authority for natural persons is at the moment established only at HALCOM-CA headquarters but it is also possible to file an application by regular mail in case that the signed application form has been certified by a notary. The Registration Authority for legal persons is established at HALCOM-CA headquarters and in a number of Slovene banks; the application can also be mailed if it has been signed and certified beforehand by a notary.

Digital certificates from HALCOM-CA can be obtained by citizens, employees and servers.

Like the prior Certificate Authorities, HALCOM-CA also issues two types of certificates:

- standard certificate has single key pair and is usually installed in web browser; it can be used for creating digital signatures and encrypting data; these certificates are most frequently used in web applications and S/MIME communication between users.
- advanced certificate consists of two key pairs: one for digital signing and the other for encrypting data; in order to use this certificate a special application (middleware) is needed; it can be used in web applications and for S/MIME communication between users.

Standard certificates are intended just for natural persons and are usually stored directly in browsers' certificate store. Advanced certificates can be obtained by natural and legal persons and they are always stored on a smartcard; in order to use them, certificate holders need also a USB, COM or PCMCIA reader. CA uses CRLs as a certificate validation system and publishes them on-line.

Every certificate for natural person contains its holder's tax ID number whereas certificates issued to legal persons contain the user's personal tax ID number and VAT ID number of a company. These data can be used by applications to establish an indubitable connection between a single certificate and its user.

AC NLB

This CSP operates two issuers of qualified digital certificates: NLB CA and AC NLB, although the first one is no longer used for issuing certificates – its only purpose is to manage issued certificates until they expire. Currently, all the certificates are issued by Certification Authority AC NLB only. Its certificates can be obtained by natural and legal persons who are clients of the bank Nova Ljubljanska banka. The intended usage of these certificates is to enable e-banking for the users. Registration Authorities for natural and for legal persons are established at all branch offices of Nova Ljubljanska banka. To get a certificate the user must file an application form in person at the Registration Authority.

Digital certificates from AC NLB can be obtained by citizens and employees if they or their companies are clients of the bank. Additionally, certificates can be issued to employees of the bank for internal usage.

This CSP issues only one type of certificates – web certificates. They have a single key pair and are mostly used in web browsers; they can be used for creating digital signatures and encrypting data; these certificates are most frequently used in web applications for e-banking but can be also used in other applications and S/MIME communication between users.

Certificates issued by AC NLB can be stored on a smartcard but can be also used as software certificates. The CSP doesn't prescribe a mandatory usage of smartcards. The CA uses CRLs as a certificate validation system and publishes them on-line.

Digital certificates contain personal tax ID number of certificate holder. This information can be used when authenticating users in applications.

POŠTA®CA

POŠTA®CA is a Certification Authority at Slovene Post. It issues qualified digital certificates to natural and legal persons but it also issues normalized certificates to other users. Since these certificates aren't qualified they can't be used in applications that follow ECESA law. Registration Authorities are established at all branch offices of the Post, where physical identification of future certificate holder is required when applying for a certificate.

Qualified digital certificates from POŠTA®CA can be obtained by citizens and employees whereas normalized certificates are issued to servers and other hardware equipment.

There are two basic types of qualified certificates available:

- a standard certificate has single key pair and is mostly used in web browsers; it can be used for creating digital signatures and encrypting data; these certificates are most frequently used in web applications and S/MIME communication between users,
- an advanced certificate consists of two key pairs: one for digital signing and the other for encrypting data; in order to use this certificate a special application (middleware) is needed; these certificates are mainly used in dedicated applications but can be also used in browsers and S/MIME clients.

Standard certificates can be either stored on a smartcard or used as a software certificate whereas advanced certificates must be stored on a smartcard. Depending on the certificate type and its storage different financial liabilities apply. For example: if a certificate isn't stored on a smartcard, the Certification Authority has just minimal financial responsibility for transactions digitally signed with such a certificate. The CA uses CRLs as a certificate validation system and publishes them on-line.

Digital certificates contain the personal tax ID number of the certificate holder. This data is used for authentication of users in different applications.

Health Insurance and Professional Card

The project of issuing Health Insurance and Health Professional Cards began in 1995, the first cards were introduced in 1998 and in 2000 all cards (2 mio) were successfully issued. The system was upgraded in 2003.

The health card is a microprocessor smartcard (16kB memory chip card, by Gemplus); HPC cards have access to data on the HIC cards by activation with 4-digit PIN code. Cards can be read on card terminals and there are approximately 300 such terminals in Slovenia.

3.3.4 Organisational aspects

As already stated the legal basis for the introduction of digital certificates and electronic signatures in eGovernment applications for administrative operations can be found in the Decree on administrative operations. According to the decree the e-government applications for citizens and private sector can be performed by any qualified certificates issued by registered CSPs, governmental CAs and other commercial certification authorities. Since the national eID cards have not been introduced yet (although the Slovenian national eID project already official started by establishing a project group) currently most eGovernment applications use authentication and digital signature capabilities based on qualified certificates from certain registered certification authorities, governmental as well as commercial. CSPs, their services and procedures used to map certificate to its holder were described in detail in Section D.3.1. The role of the National Register Number and Tax number, two of the building blocks of the Slovenian eGovernment authentication/signature strategy was described in Section C.3.2.

3.4 Interoperability

Qualified certificates - cross border ***regulatory issues:***

Qualified certificates issued by certification-service-provider with its seat in the European Union are equal to Slovenian qualified certificates. Also qualified certificates issued by certification-service-provider with seat outside European Union are equal to Slovenian, under the following conditions, i.e.:

- in case such non-EU certification-service-provider fulfils conditions defined by the Electronic Commerce and Electronic Signature Act, is voluntarily registered in Slovenia or other EU state; or

- in case the bilateral or multilateral agreements between Slovenia and other state or between European union and other states define so.

*Qualified certificates – cross-border **in practice:***

There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements). Until now no interoperability measures have been implemented.

eHealth:

At present solution no interoperability measures have been implemented.

Interoperability is precondition for free movement of health professionals, EU citizens and health care services; in the upgrade of the HIC and HPC system we intend to incorporate all relevant recommendations available at common market, like standards for electronic EU HIC, HPC, ….

3.5 eIDM Applications

Generally speaking, e-government applications can be based on different identifiers (i.e. Personal Registration Number or Tax Number). Since eIDM systems use only a subset of all possible identifiers, a translation between them is necessary in order to enable users to access certain applications with certain eIDM tokens in case that they don't share common identifiers. Below there are shortly described some e-Government applications that use digital certificates for authentication and/or digital signature. It is important to mention that every application must use a proper certificate validation service (depending on the issuing CA) in order to ensure validity of a single user certificate used for authentication or digital signature.

e-SJU portal

e- SJU stands for electronic services of public administration portal. The portal e-SJU offers a single access point for all forms that can be published on the web by any public administration institution. The forms are published in different formats, which can be filled in by citizens and sent to the selected institution. The administrative taxes and other costs related to the service can be paid through the e-SJU portal by credit and debit cards, by using mobile methods of payment, and through online banking. The application forms submitted by users over the e-SJU portal can have a different authentication levels (see D.1.3.) Users can find in a single point the description of the services offered by public administration institutions and corresponding forms, needed for operating with public administrations. Users can therefore perform all operations with public administrations in a completely electronic manner. Currently, the system includes the description of over 400 different services and 350 forms, but not all public administration institutions are included in the system. By increasing the number of public administration institutions to participate in the system the offer of information and services will increase. The goal is to have all 6000 public administration institutions in Slovenia participating in the system in the future.

e-Taxes

The application e-Taxes supports filling out and secure filing of tax forms – a list of currently supported forms is published on the application web page. The whole process consists of filling out a form, validation of data, filing a form by digital signing and time-stamping it. The application also allows taxpayers to calculate the amount of their tax and import or export their data.

Authentication (and digital signature) are based on qualified digital certificates. The system of mandating integrated within the application allows tax payer to mandate a user for filing tax forms. Each user (end user or mandated user) must register before the first usage of the application.

One-Stop-Shop - State Portal for businesses

The One-Stop-Shop portal enables a natural person to register his/her business activity in the Business Register and transfers a person’s tax data to the Tax Administration. At the same time the user is able to register his and his under-aged children’s health insurance.

Besides business registration other procedures can be performed through the portal:
- business data changes (written to Business Register),
- deregistration of business activity,
- application for other user’s data from Business Register.

The resolution on business registration can be delivered electronically.

EPOS

The application EPOS is a cornerstone of a centralised information system of Slovene Customs. It supports collecting and controlling of different customs declarations. It enables on-line communication between all members of the process: reporting units of companies, accredited companies and companies that offer commercial programming tools for reporting customs data. The system is a central module that accepts declarations, verifies digitally signed messages and routes them according to their content to a dedicated application. It also digitally signs replies to received data.

Currently there are 5 back-end applications that support different customs procedures and (will) make use of the EPOS application:

- SICIS (Slovene Customs Information System): the application is intended for receiving customs declarations and sending replies; at the moment it supports only simple declarations but later other kinds of declarations, too; it is operational since1.1.2007,
- NCTS (New Computerised Transit System): the NCTS application has been developed to allow transit declarations to be done electronically in compliance with the European regulatory framework; the application is in development phase,
- AES (Automated Export System): the application is in specification phase,
- AIS (Automated Import System): the application is in specification phase,
- EMCS (Excise Movement and Controlling System): the application is in specification phase.

Authentication and digital signature are based on qualified digital certificates. Each user (reporting unit or accredited company) must register before the first usage of the application.

Annual Reports

The agency AJPES is accredited for management and publishing of annual reports data. These reports include data on performed business and financial situation of a single business entity. The Agency collects data with two intensions:

- to enable public access to these data,
- to carry out statistical and analytical researches (for state statistics).

The Agency prepares and manages databases of annual reports for several years. Users can obtain collected data on an individual basis in certain range and content according to Slovene legislation on information availability; complete, unlimited data are available only on an aggregate level (i.e. on a state level, for all business activities or statistical regions).

Business entities fill out the corresponding form and file it to the Agency electronically through the Agency's web portal. Following types of business entities can report business data through the application:

- companies,
- natural persons doing business activities,
- societies and other non-profit organizations,
- public institutions.

Structured data can be imported in the XML format and unstructured data in the PDF or TIFF format.

The digital signature is based on qualified digital certificates. Each user must register before the first usage of the application.

E-business in agriculture

The application provides a basis for a centralised information system of the Agency for Agricultural Markets and Rural Development. It supports secure filing of data of a different kind i.e. applications for direct payments. The system is a central module that accepts filed data, verifies digital signatures and routes messages according to their content to a dedicated application. It will digitally sign replies to received data.

There are 5 modules in the centralised system:

- main portal: all back-end applications are connected through this portal; it is used for user authentication, too,
- digital signature: this module is installed locally and enables users to digitally sign web forms,
- user module: it supports user identification and authorization,
- web administration module: it is based on user module functionalities and is used for web administration of users,
- e-archive: all filed documents are stored in this module; it also takes care for digitally signing and time stamping of received documents.

Authentication and digital signature are based on qualified digital certificates. The system of mandating integrated within the application allows a farm owner to mandate a user for filing his/her forms. Each user (end user or mandated user) has to register before the first usage of the application.

3.6 Future trends/expectations:

Introduction of Slovenian e-ID card

Slovenia has started to develop electronic identity (e-ID) cards in February 2003 (the ID card in Slovenia is not obligatory); nationwide issuance of e-ID's was planned for 2005, but was postponed for at least 3 years. The Slovenian e-ID card concept is to be the combination of a signature card and a conventional, visual ID-card. Individuals will be required to request a Slovenian e-ID card at a registration authority or an administrative office. As with the present ID card the individual must be registered with the central population register (CPR), thus the individual will have her personal registration number (PRN) already. Based on the personal data the e-ID card will be personalized. A certificate serial number (SN) will be stored in a special database along with the PRN.

From a technical point of view, the smart card of the e-ID card shall hold:

- personal data of the card holder, such as name, etc.
- two key pairs thus two electronic certificates: one certificate/key-pair for authentication and encryption purposes, a second certificate for creation of electronic signatures.
- Upon latter decision the card should be ready to contain additional biometric data.

Besides providing an electronic identity, the Slovenian e-ID card shall be used as conventional ID card as well. Therefore, the layout of the front side is to contain the cardholder's personal data and her/his image.

The health insurance card: **the renovation for on-line access to health insurance data**

The final goal of the renovation of the health insurance card system is to have a fully operational on-line system where the new health insurance card and health professional card no longer store data but instead only the certificates allowing direct access to the data.

Currently, the health insurance card stores data on: compulsory and voluntary health insurance, personal physician, issued medical and technical aids, and issued medication. The above are the priority candidates for implementation of the new system, i.e. direct data access. Provision of on-line access to these data means building the necessary secure infrastructure at the Institute and upgrading the IT solutions on the providers' end.

The first stage of on-line access therefore involves access to data now stored on the health insurance card. This will ensure that the data are up-to-date and it also allows for the existing set of data to be expanded (e.g. adding temporary and permanent residence, name of the medication and medical aid next to its code).

The following functionalities will be gradually introduced in subsequent stages of establishing on-line access:

- electronic prescription,
- insurance holder's access to his own health and insurance-related data,
- access to analytical data for health insurance purposes,
- other electronic health insurance documents.

The infrastructure established in such a way will also provide an important basis for accelerating the development of the electronic health record, exchange of health records between healthcare providers and introduction of other applications for use in expert medical work within the Slovenian healthcare system in accordance with the Slovenian eHealth 2010 strategy.

The renovation will be divided in the following phases:

Phase 1:

- Introduction of the new generation of health insurance card (HIC) for the insured persons and new generation of health professional card (HPC) for the professionals in health care and health insurance. HPC will carry qualified digital certificate for the on-line access to the health insurance data.
- Development of infrastructure for the on-line access.
- Development of the e-prescription prototype solution.

Phase 2:

- Development and employment of the e-prescription at national level.
- Development of other e-applications using e-signature on the HPC and/or HIC.

The introduction of the new HPC, HIC is planned in the middle of 2008, with a gradual introduction of on-line accesses to follow from April 2008.

Details on this: http://www.zzzs.si/

3.7 Assessment:

Slovenia will strive to advance the progress of eGovernment, according to both the established comparative criteria of the EU and the less measurable but still exceptionally important results of eGovernment: user satisfaction, reduction of administrative burdens, innovative solutions, new business models, co-operation with various persons and other countries, the implementation of good practice, the forming of a knowledge database, rationalisation of internal operations, qualification of all participants for the use of eGovernment, standardisation and central management of eGovernment, interoperability etc.

To speed up the rate at which on-line public services are made available for citizen and companies several steps have already been made. As stated in Slovenian eGovernment Strategy national interoperability framework is needed to attain the planned development of eGovernment until 2010. SEP-2010 defines an interoperability framework as linking of all elements (standards and recommendations, uniform architecture, open standards and solutions, guidelines), including eID and authentication methods in a national interoperability framework for eGovernment services and solutions, which will provide organisational, semantic and technical interoperability and at the same time creative co-operation in the preparation of an interoperability framework for cross-border European services.

The legal basis for the introduction of eIDM systems in eGovernment applications for administrative operations can be found in the Decree on administrative operations (Official Gazette of the Republic of Slovenia, No. 20/2005, 106/2005, 30/2006, 86/2006). According to the decree the e-government application for citizens and private sector can be performed by any qualified certificates issued by registered CSPs, governmental CAs and other commercial certification authorities. Unfortunately, the national eID cards have not been introduced yet. A Slovenian national eID project officially started in February 2003 by establishing a project group, but the project was suspended. But it is expected that the project will roll-out again in 2008.

With regards to the global objective to implement an EU wide interoperable system for the recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State we support different activities for cross border eIDM recognition. The Member states already have sometime eIDM infrastructure. We support the model of interoperable eID mutually recognised in all Member States, while keeping their systems and practices thus ensuring compliance with the subsidiarity principles. Every MS should have the ability to adopt its own technology, policy, and platform.