IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE CZECH REPUBLIC

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 eGovernment applications in the Czech Republic.

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

Until now, there is no general eIDM system in the Czech Republic. If an administrative body wants to use identity management in an electronic form, it establishes a new eIDM system ad hoc.

Citizens in the Czech Republic are identified to administrative bodies based on personal identity numbers – it doesn't matter if the identification is done in paper or electronic form. This number (with other data about a person) is administered through the Population Register (this register is sometimes known as Register of Residents and Birth Numbers, a central register managed by the Ministry of Interior, http://www.mvcr.cz/ministerstvo/povinne/iseo.html).

Sometimes qualified certificates issued by accredited certification service providers are used with for eIDM purposes. Qualified certificates typically use no personal identity number, although it is possible to have a social security number in the qualified certificate (if a citizen wants to use a qualified certificate to sign electronically in communication with a public administration, this identifier must be present in the qualified certificate). This identifier is stored in the information system of the state social assistance managed by the Ministry of Labour and Social Affairs (http://portal.mpsv.cz/soc/ssp).

In the Czech Republic, approx. 40 000 valid qualified certificates have been issued (statistics for year 2006 - http://www.micr.cz/images/statistiky/epodpis.pdf) and almost all of them contain the above mentioned social security number (on a population of 10,3 million, it is a relatively low number). Some qualified certificates are stored on smart cards (statistics are not available), but this is not mandatory. Most of the qualified certificates are software based. The current trend is a doubling of the issued certificates every year. Certificates are mainly used by employees of private companies and public administrations. There are 3 accredited certification service providers that issue qualified certificates.

There is no eID card in our country, and our political representation doesn't support this type of possibility of entity authentication.

A key problem with the personal identity number in electronic communication is that it is possible to find this number on Internet for some people, and that it is also possible to guess it, because this number is constructed from date of birth and sex of the citizen, and 4 added numbers.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

In the Czech Republic there were many attempts to establish eGovernment in the sense of something strategically centrally coordinated, but in reality it is not yet well coordinated on a central level. eGovernment is created by many applications developed in different ways by public administration bodies – this is not a coordinated process but rather a natural growth of applications of resorts that depend on activities of responsible persons in those administrative bodies.

This is the reason why eGovernment is successful mainly in tax, social and health security, land registry rolls and customs. The only step taken to coordinate those applications was the building of a Public Administration Portal, from which all those services are accessible. However, all of those applications use different ways to identify their users, etc.

eGovernment projects should be coordinated by the Ministry of Informatics, but in reality it didn't have sufficient power, as it couldn't decide on the financing of eGovernment projects. As a result, the other administrative bodies created their projects independently of the wishes of the Ministry of Informatics. Reality is that on 1 June or 1 July 2007 the Ministry of Informatics will be closed and its competencies in the field of eGovernment will fall under the Ministry of Interior.

There is no federal or regional subdivision in our country. There is only local government, but there are no materially successful local eGovernment applications. The only future eGovernment application on a regional level will be "land-use planning", but these information systems are in the very early stages. Coordination of local government falls under the competences of the Ministry of Interior – but eGovernment isn't a real priority of the activities of this Ministry. The Ministry of Interior created the portal e-PUSA to collect and publish information about local authorities - http://www.epusa.cz/ (only in Czech).

Generally there are 3 central registers (the Central Population Register, the Register of Companies and the Register of Land and Addresses) – but the communication among registers is not very sophisticated. The law on Data Sharing between Administrative Bodies has been proposed (as it is written on MODINIS IDM study website https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/CzechProfile) which aimed to establish rules for data sharing, communication between registers etc.; but this law was not accepted because of legislative mistakes in this act. Now modifications of this act are being drafted, some parts are added and the whole document has been divided into two acts – the Act on Electronization of some Processes and the Act on Registers. Those acts are in the draft phase and there are many comments from stakeholders to those acts – currently it is impossible to guess how it will finally be.

3.2.2 Traditional identity resources

For identification purposes, in the Czech Republic one traditionally uses a personal identity number ("*rodné • íslo*" – "birth number"). This number is used primarily in the "paper world", and has been allocated to citizens since 1950. Because this number is practically used as primary identifier in almost all governmental registers and databases, this number is used for identification also in electronic form. True is, that even though there exist name/password identification systems or other identifier systems, in the end citizens are always identified by this personal identity number. For the purposes of demonstrating their identity, the number is combined with a paper identity card or usually with a qualified certificate in electronic form (which is not a good practice, but has already happened).

In the central population register (the central register managed by Ministry of Interior, http://www.mvcr.cz/ministerstvo/povinne/iseo.html) the personal identity number is administered. A Czech citizen gets this number after his birth. If a foreigner also wants to get this number, he must apply for it – but since it is part of the content of a residence permit, the foreigner usually only gets this number when acquiring a residence permit.

The data collected about Czech citizens are a little bit different to data collected in Population Register about foreigners. A list of this data can be found on the above mentioned website (unfortunately not in English). Primarily for Czech citizens the data includes all names, date of birth, personal identity number, gender, place of birth, citizenship, permanent residence address (including all official residences in history), beginning and end of permanent residence and esp. end of permanent residence in Czech Republic, incapability to legal acts, prohibition of residence, place of this prohibition and time of this prohibition, personal identity number of father and mother, marital status, place of marriage/registered partnership[3], personal identity number of husband/wife/partner, personal identity number of children, data about adoption of children, record of data provision from register (date, time, to whom it was provided), date and place of death.

For foreigners this information includes (in addition to the information for Czech citizens) a citizen number and validity of residence permit, beginning and end of residence, data about deportation, and data about specified related persons.

The documents containing a personal identity number are the birth certificate, identity card, passport or residence permit (http://www.mvcr.cz/rady/kompletni/rod_cis3.html). For authentication purposes, citizens primarily use identity cards or residence permits.

The identity card contains at least surname, given names, date of birth, gender, personal identity number, nationality, date of expiry, document number, photography, signature of holder, machine readable text, place of birth, permanent residence address, maiden name, marital status, date of issue and issuing authority (of course there are security components like hologram..). There could be

[3] it is possible to become registered partner also when a citizen is homosexual – then it is possible in some cases to have the same rights as a husband/wife, e.g. to get access to health documentation.

academic titles and names of husband/registered partner and children. The card is mandatory from age of 15. The residence permit content is similar to identity card.

The central population register contains information about all citizens. If a foreigner applies for a residence permit, his record (and personal identity number) will be created in the population register.

Every citizen has the right to obtain from the population register information which is saved there about him if he applies for it. The data are saved for 50 years after the death of the person. This register is operated in accordance with the Act on the population register and personal identity numbers, No. 133/2000 Coll., *zákon o evidenci obyvatel a rodných • íslech*).

There is also an identification number for economic entities that is not centralized in a single register, but which is kept in the Companies Register (a central register managed by Ministry of Justice, http://portal.justice.cz/uvod/JusticeEN.aspx; the data are provided to this register by Register courts), in the Trade Register (http://www.rzp.cz/, a central register managed by the Ministry of Industry and Trade, data for this register are provided by Trade Licensing Offices), in the Economical Subjects Register (central register managed by Czech Statistical Office, http://dw.czso.cz/rswj/dotaz_en.jsp); and in 120 another small registers of different types of enterprises. The best practical way how to find correct information about legal entities is to use the register/application of the Ministry of Finance ARES - http://wwwinfo.mfcr.cz/ares/ares.html.en, the Administrative Register of Economic Subjects. This Register and Application of the Ministry of Finance makes accessible the data from all above mentioned resources. All registers of economic entities are publicly available. It is possible to get official output of this registers in paper form in some offices (local government offices). There is a plan to create one register from these 120 registers, that will be called Commercial Register – but this is really long-term plan because it requires many changes.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

In the field of central registers the Czech policy is changing. As written above, economical subjects could be in 3 registers and the data of those registers are based on paper data in many offices. This has to become one Register of Subjects. The Population Register also has problems – data there are often incorrect and it will take many years to clear these mistakes. This is a big problem for applications, such as e-voting, because it has to rely e.g. on the correct residence address of the people. Then there is the Register of Land and Addresses – but this register identifies places, not persons, so it’s outside the scope of this study.

No authentic source principle has been implemented yet, but there is a will to implement it (the above mentioned Act on Data Sharing between Administrative Bodies - *Zákon o sdílení dat p•i výkonu ve•ejné moci* was intended to implement it, but as mentioned before, the act wasn’t accepted – but there are another drafts of acts that will implement this principle).

There is no globally used eID card present in Czech Republic and there is not any project or political statement saying that there will be eID card for citizens. As mentioned in chapter B., it is possible to have qualified certificate (respectively private keys) on smart card, but most users use “software based qualified certificates”. Qualified certificates contain the social security number.

There is a plan to establish a new system of identifiers inspired by the Austrian model, to be implemented by an “e-government act”. This act is now in draft phase. In this plan it currently seems (the plan is still subject to very hard discussions) that citizens (mandatory only for representatives of legal entities) will have a source identifier on a “technical carrier”, and from this identifier some central service will derive an “agenda identifier” which will be the unique identifier of the person in one context and it will be different in another context. This has to disallow clerks of public administrations to access data which do not belong to their competence. This plan is not very sophisticated yet; there are many things which have yet to be solved.

There are basically 3 practically used systems for entity identification/authentication used in electronic communication when using eGovernment services (see below for more details on all systems).

- The first is a name/password/advanced electronic signature system – the name is connected with a qualified certificate (serial number) used to sign data that the user sends to the system. This name/password is issued only for usage in one application (every application has its own system of issuance of name/passwords). This system is used in communication with The Czech Social Security Administration, Ministry of Agriculture etc.

- The second is the usage of a social security number – the problem is that only the Ministry of Finance has access to the service of Ministry of Labour and Social Affairs which compares personal IDs and social security numbers (it is not allowed to use this number in any other way according to state social assistance act, No. 117/1995 Coll., zákon o státní sociální podpo•e). The Ministry of Justice plans to use this system for the issuing of extracts from the Penal register.

- The third one is that a communicating person must enter his personal identity number (or other data sufficient to uniquely identify person) or identification number of economic subject in a form which is electronically signed. The identification is made only through the connection of data from a qualified certificate and the personal identity number in the signed form. This is used in customs declaration applications and in usual communication with public administration. In some cases the serial number of the qualified certificate is enough for authentication purposes as the identifier of the person for the type of application.

There is no authentication policy in Czech Republic – every administration body is doing it its own way, as it is written above.

Regional/local applications using authentication of citizens are not present at this time – if they will be, they will again be different from application to application.

Generally it is possible – and in fact since 1 January 2007 it is mandatory (although almost no one fulfilled this obligation) to provide information on the accessibility of public administration information systems into a centralised information system (https://isdp.ext.micr.cz/isvs/). One of the data filled out in this system relates to the information system's security policy containing security measures such as conditions for identification & authentication to the application. So using this centralised system it is possible (or it will be, after the system has been filled with more data) to get information how to authenticate in any public administration application.

3.3.2 Legal framework

Main legal provisions on personal identification:

- The Act on population register and personal identity numbers, No. 133/2000 Coll., (*zákon o evidenci obyvatel a rodných • íslech*);
- The Ordinance on the implementation of the act on the population register modifying ordinance No. 177/2004 Coll., on the implementation of the act on the population register, the act on identity cards and the act on travel documents, No. 296/2004 Coll., (*vyhláška, kterou se provádí zákon o evidenci obyvatel a kterou se m• ní vyhláška • . 177/2000 Sb., kterou se provádí zákon o evidenci obyvatel, zákon o ob• anských pr• kazech a zákon o cestovních dokladech*)
- The Act on identity cards No. 328/1999 Coll., (*zákon o ob• anských pr• kazech*)
- The Civil Code, No. 40/1964 Coll., (*ob• anský zákoník*)

Main legal provisions on legal person identification/registers:

- Trade law, No. 455/1991 Coll., (*zákon o živnostenském podnikání*)
- Commercial code, No. 513/1991 Coll., (*obchodní zákoník*)
- There are 135 acts which are concerned in some way with the competences of public administration bodies connected with identification of legal persons – this was subject of a study of commercial registers available at http://www.micr.cz/scripts/detail.php?id=3485 (in Czech language, list of legal provisions is in the first attachment)

There is not any act determining how one should identify when using eGovernment applications. An "e-government act" is planned which will state that a citizen must identify himself based on a source identifier and that the public administration must be able to use this system. In the plan this system of authentication will be mandatory for electronic forms of communication – but it will not remove any paper form of communication (citizens must have the possibility to get the required services in "paper form"). Electronic communication will be mandatory for public administrations (ministry to ministry must send documents in electronic form), and they have to use the source identifier in their authentication processes.

The legal framework for signatures is already working (also legislatively everything has been created) and public administrations use the electronic signature. There is no authentication legislation in force. The solutions of authentication are application specific, because there is no legislation saying how to authenticate generally (although there are no acts saying how to authenticate in specific applications either; there is only a technical solution in such cases). Probably this should be prepared – and there will have to be a similar act on e-authentication as there is already on e-signatures. It currently seems that there will be legislation requiring authentication, before any legislation saying how to authenticate. This is not good, but if the first step can push the whole process, finally it could work properly.

The personal identity number is legally protected by Act No. 101/2000 Coll., on the Protection of Personal Data, *Zákon o ochran• osobních údaj•*, because the number itself is constructed from the date of birth and the gender (it is easily possible to find out this data from personal identity number), which is of course personal data.

The systems which are commonly used in public sector applications, apart from the system using the social security number, could be used in the private sector in the same way as it is used by public administrations – that means, without any legislative support.

A legal entity can be represented by the natural person who is the statutory representative (this information is noted in the Companies Register). In some cases it is possible for a representative of the statutory representative to act – but this then works the same way as in "paper form". This person must fill company identification number and authenticates himself as required by the application.

3.3.3 Technical aspects

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

There is combination of systems (a,d,e) – because there is no established real eIDM system (there is no official eIDM system) – the authentication system is different from application to application. Often the authentication is combined with a need to send the personal identification number in the communication by the citizen (but it does not exist in any form from above mentioned foms).

- *If any, which is the token format chosen in your country IMS?*
    - *a) Token format is ID1 (e.g. "credit card" format)*
    - *b)* **Token format is ID2 (larger (A7) format) (but without electronic means)**
    - *c) Token format is ID3 (passport format)*
    - *d) Other (USB tokens, etc. – please explain)*

Because there aren't any plans yet to establish a real standardized eIDM system in our country and there wasn't expert group trying to define technical solution, the next questions in questionnaire aren't relevant. No significant decision has been made yet, and the work hasn't even started. There are no requirements on token/data storage of any data used for authentication.

In the Czech Republic the electronic signature is often practically used for authentication (it is not real authentication, it is identifying of a person after signing data). It is not possible to use a qualified certificate e.g. in SSL protocol authentication in the Czech Republic, because the signing person must see what she is signing (WYSIWYS rule). But public administrations use the properties of a qualified certificate, because it is the most widespread form of information usable for identification.

In the Czech Republic it is possible to have software certificates. There are 3 accredited certification service providers, but only one of them also issues smart cards (but it is also possible to get software certificate from this certification service provider). Almost all certificates in the Czech Republic are software certificates.

3.3.4 Organisational aspects

Because there is no centralized eIDM system, the three above mentioned systems will be described. Electronic identity management is application specific in the Czech Republic – every application has its own. It is hard to generalize some characteristics of electronic identity management.

There are however some general rules which are true in all mentioned cases.

All these applications have been created by a central public administration body, and data in the system is available only to that central public administration body. Sometimes the data is also available to hierarchically underlying public administration bodies (e.g. Ministry of Finance provides these data to corresponding Revenue Authorities). These applications are not interconnected.

It is possible to use web client applications and/or special client applications supporting communication with the application server in all cases (i.e., the public administration makes data structures publicly available that are accepted when sent to the server as well as the data structure of their responses to the client application, so it is possible to implement communication functionality into commonly used applications). Usually when the user wants to use a web client he must apply a user account before he can use the web client. Public administrations usually publish a list of software (client applications) which supports this type of communication.

Federated identities are used only if it is useful for given type of application.

In all cases it is possible to use a qualified certificate issued by an accredited certification service provider, but it must typically be completed with some other properties.

Name/password/advanced electronic signature based on qualified certificate

In the first system - name/password/advanced electronic signature –, a person must have a valid qualified certificate (issued by a qualified certification service provider). Then, she exports it and takes it to the office of the administration body which provides the service/application. At this office her identity is verified and she receives authentication data about her registration to the system (after registration to the application she may change/create her password). The administration body holds in its database the personal identity number, serial number of the qualified certificate, name of certification service provider and number of user account of this person. Thereafter the person can communicate with the administration body – with usage of identifier/password and qualified certificate.

Federated identities are used only partly – it is possible to use the same data for authentication in more roles (these applications are mainly for enterprises and the person can represent more companies). But it is not possible to use the same data for authentication in applications created by other public administration body (it is only possible to use qualified certificate).

Every company has the right to manage its own roles in the application. All persons/users must pass the registration process.

There are software tokens - qualified certificates issued by a qualified certification service provider (in the Czech Republic qualified certificates needn't be on hardware token/smartcard) and registration data issued by public administration body that maintains the application.

The information is verified by public administration body that provides the application and this body is also responsible for any errors (although the user is partly also responsible, since he has to take care of his data).

Social security number in qualified certificate

The second is usage of social security number (it is called ID MPSV) from a qualified certificate. The user must have a qualified certificate with his social security number (this number is in the field Alternative Names/Other Name/MPSV – registered with OID 1.3.6.1.4.1.11801.2.1). Because this identifier is used in most e-government applications, accredited certification service providers usually recommend signing persons that it is good to have this number in the certificate (almost all certificates are issued with this number).

Signing person must apply for the social security number and the certification service provider sends an electronic application with the personal identification number to the Ministry of Labour and Social Affairs, that sends back the ID MPSV (this is a service provided by the Ministry of Labour and Social Affairs to all accredited certification service providers). If the signing person didn't have an ID MPSV, a record of that person is created in the database and a social security number is generated for her.

The system of the Ministry of Finance that uses this type of authentication changed a little bit and a person can now also apply for establishing a tax information box, where she has access to all her (or her companies) tax data – but this is only a superstructure of the basic system. This application is sent electronically, it is electronically signed based on a qualified certificate and after 15 days the tax information box is established by the Ministry of Finance. Any authentication in this system is based only on a qualified certificate and the social security number.

Federated identities are used only for this type of application (if the same type of authentication is used). It is possible to use the same qualified certificate in all e-government applications (but sometimes it isn't enough, depending on the requirements of the application).

In this type of applications there is no role management (it is not possible because of the characteristic of these applications).

Only qualified certificates are used, which could be software or hardware tokens as mentioned above.

Identification number and qualified certificate

The third system is that a communicating person must write its personal identity number (or other data sufficient to uniquely identify the person) or identification number of the economic subject in a form which is then electronically signed. The person must have a qualified certificate and a personal identity number (or just an address, company identification number, or license number).

If a person wants to use the service, she only uses applications supporting this type of authentication (web based or an installed client) and signs a form where all required data is filled out (including identification data). The person sends the signed form and data to the service provider/public administration body. Because the information is signed in a trustworthy manner, it is possible to trust the information.

Generally it is possible to use communication via the usual e-mail client. The person must provide enough information to be "identifiable" for the public administration body. If the person is "identifiable" the public administration body must deal with the problem that the person has (e.g. start and finalise any administration procedure).

Qualified certificates are used, which could be software or hardware tokens as mentioned above.

The provider of the specific application verifies if the data in the form corresponds to the data in the qualified certificate and in his database. This is done by automatic process or manually (in above mentioned general case).

If the person fills the form with incorrect identification data, this is considered an attempt to fraud and the person is responsible for it. If a public administration body verifies the information incorrectly, it is responsible for the mistake.

3.4 Interoperability

All above mentioned systems are accessible to holders of qualified certificates issued by an accredited certification service provider. In practice it works only for qualified certificates issued by an accredited certification service provider from the Czech Republic.

In case of the system with authentication via name/password/qualified certificate authentication a person must go to the office of a given public administration body, which is also in the Czech Republic (but it is possible to get the required data also if the person is non-national). After the person gets this data, she can return to her country and authenticate with it.

In case of the system based on social security number in qualified certificate the person must apply for social security number and Ministry of Labour and Social Affairs creates it also for non-nationals.

In case of the system where some kind of identification number is used, this number is issued after fulfilment of given conditions. These conditions differ from application to application, but may require a visit of some public administration office.

Conclusion is that it is possible to be included in all mentioned eIDM systems also as non-national, but the person must go to the Czech Republic for a qualified certificate and in some cases also for other registration data.

There are currently no plans to make eIDM systems in the Czech Republic interoperable with other countries (including the system which is in the planning stage based on the planned new e-government act). Plans are currently more concentrated on the solution of internal problems. Because the planned solution is based on solutions in other EU countries it may be theoretically interoperable with the other solutions. There is also not a very strong focus on the interoperability of eIDM system because most of the applications are used by Czech nationals.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems in the public sector. There are not many applications where electronic authentication is used in the Czech Republic.

Private sector applications use thei own way of authentication – but this is also because there is no general model and service for eIDM, only application to application solution of authentication.

3.5.1 Name/password/advanced electronic signature based on qualified certificate

This type of authentication system is used in submissions of employers for pension and health insurance to the Czech Social Security Administration (http://www.cssz.cz/epodani/epodani.asp). A total of 13 million documents were sent through this application, but since enterprises must send lot of documents for every employee, the number seems very high. A more significant number is that it is used by 66% of enterprises with more than 25 employees, but also by 21 thousand small enterprises.

Another application with this type of authentication is the farmer portal (https://farmar.mze.cz/EPO/EPO_INDEX.html).

3.5.2 Social security number in qualified certificate

The main application for this system is the tax portal (http://adis.mfcr.cz/adistc/adis/idpr_pub/dpr/uvod.faces). A total of 40 500 submissions were sent in 2005 and 91 408 submissions in 2006 (to illustrate the growth, but it of course should be higher).

Another application using this form of authentication is the application for social allowances (https://forms.mpsv.cz/sspforms/OutlineForm.jsp?Type=List&L=en) (statistics aren't available but this application is not very used, because of the type of application).

3.5.3 Identification number and qualified certificate

E-customs applications represent the majority of this type of applications (there is needed only identification number of the legal entity and qualified certificate, http://www.cs.mfcr.cz/CmsGrc/Clo-online/) – this application is used very much; in some types of transport it is used almost in 100% of declarations.

3.6 Future trends/expectations

In the Czech Republic the situation in this field is changing and political representation hasn't yet decided on the way of identification and authentication in electronic world.

Currently it seems likely that we will have new source personal identifiers which will be stored on smart card. However, this smart card won't be a personal ID card. Every legal entity (respectively person representing the legal entity) will have an obligation to get this smart card or another technical device in which will be stored a source personal identifier. For other people it will be voluntary to have this identifier and technical device.

The old personal identification number will not be removed by source personal identifiers. Truthfully, because of the personal identification number format it has been calculated that in 2053 it will not be possible anymore to issue this type of numbers – although other solutions are conceivable, such as adding one number. But this is really over a very long period of time.

A central system should be established which will be able to derive from this source number a personal identifier for given sectors. This central system will provide authentication service for all sectors.

There is also a plan to rebuild the central registers, because there are many problems with duplication of data, there are many mistakes in existing registers and registers don't communicate together well.

Work on this project will be very hard and long and must have strong political support because it costs lot of money.

3.7 Assessment

eIDM infrastructure in the Czech Republic is on the minimum possible level, but still it is possible to authenticate persons with available instruments. The system has to be improved to be more comfortable for users/citizens and government.

From a different point of view – nowadays users are used to existing applications and every change brings them more work and costs. But existing applications are also changing, and users get used to it.

There is a problem in the Czech Republic that there exists a global opinion that the common usage of electronic signatures is authentication, and it is very hard to explain that electronic signatures should be used only for signing. As a result there is little pressure to create here an eIDM framework and maybe issue eID cards.

3.7.1 Positives

- Freedom in implementation of any solution of authentication (there is not any legal act saying that it is possible to authenticate users in only one way).

- Today existing solutions work well. The used authentication systems have been implemented and systems are stable.

- Successful systems are user friendly.

- This system is very cheap for the end user. He must only have a computer, an internet connection and 7 EUR per year for a qualified certificate.

3.7.2 Negatives

- There is no authentication service that could be easily used in any application that is developed now. Maybe new application development could be less expensive if this service were available.

- The system is not interoperable between applications (a user must have different means for authentication in every application).

- Low number of possible users, because they must undertake a lot of actions to use one system and yet more actions to use another system.

- Another problem is that the legislation doesn't encompass electronic authentication (doesn't say how to reliable identify a person). Without this it is impossible to create some e-government applications, e.g. e-voting, extracts from the register of crimes.

- Some applications cannot be developed because of non-existence of eID cards (but it is not such a hard problem).

- There is a problem with incorrect data in the population registers – these mistakes must be corrected if there is to be any trustworthy eIDM system.

- The personal identification number is not as secret as the registers supposed. It is possible to abuse some personal data (but not so easy, still the systems are protected).

- The system is not interoperable with eIDM systems in EU (but especially this problem will not be solved by planned changes).