eID Interoperability for PEGS

NATIONAL PROFILE HUNGARY

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 Hungarian 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

There is a growing need for identification of users while accessing eGovernment services as more and more electronic government services become available, however at the present there is only a limited justification for the use of advanced level eIDM tokens for the purpose of authenticating private entities.

The administration already extensively uses a central identification system called the Client Gate (part of the Central Service Provisioning System). This system is a single-sign-on identification gateway through which Hungarian citizens can access all existing central eGovernment services and more and more of the local authorities' electronic services with one set of identifiers. The Client Gate became operational in 2005 and by July 2007 had more than 500.000 users. The system is developed and operated by the central administration (Prime Minister's Office Electronic Government Centre – EKK – www.ekk.gov.hu) in order to reduce the implementation cost of identification systems in the administration and to create a user friendly one-stop-shop eGovernment environment which in this case is created by the fact that Hungarian citizens can access every central government and more and more local government electronic services with 1 username-password pair through the gateway.

But we have to see that a single-sign-on system is not a username-password system; the emphasis is on the user's need for only one set of identifiers, which can also be a PKI authentication certificate. By a recently published government decree (The decree about the Central Electronic Service Provisioning System) every public authority except for local authorities is obliged to connect to the Client Gate when the service that the authority provides requires electronic identification. The goal with this policy is to ensure that the Hungarian eGovernment identification environment doesn't get fragmented and citizens can access eGovernment services at one place with one set of identifiers. Connection for local authorities is optional; but since local authorities also feel that connecting is useful for them, the number of connected local authorities is also growing. Also the earlier mentioned government decree creates a possibility for non governmental organisations to connect to the system.

In order to create the basis for a higher level (more secure) authentication (which is PKI based authentication with a chip card as the carrier of the PKI keys) the specifications of the Hungarian ID smart card interface **HUNEID** was published in July 2005 together with multiple technical recommendations about the usage of PKI technology in the administration.

The separate authentication certificate as a certificate with different legal effect than the signature certificate has not been introduced in Hungarian legislation yet. In the mentioned technical recommendations it appears that from a technical point of view its usage is possible, but the underlying legislation is missing. Recently signature certificates are used for authentication by filling out and signing forms containing identification information. The form itself doesn't have (mustn't have by a government decree) hidden content so from this aspect the usage of signature certificates for identification is not problematic; however for pure challenge-response authentication the usage of authentication certificates is needed since in this case it is not possible to solve the authentication without the signing of hidden content.

The electronic authentication of private entities in back-office processes to the public administration bodies can be carried out – by those authorised to do it – by accessing the authentic central registers online. In Hungary the data of private entities are stored and managed in the following official basic registers:

1. Register of personal and address data
2. Social security register (health and pension fund)
3. Tax register
4. Company register

The basic registers use a mathematically generated unique identifier which is a sectoral identifier and besides that they store the natural identifiers (name, place and date of birth, mother's name) of the person involved also. The so called 'personal identification number' was introduced before the Change (1989) in order to help to keep the records of public administration databases up-to-date. But in a decision made in 1991, the Constitutional Court has ruled that the general, uniform and uncontrolled use of the unique personal identification number in use since 1986 should be considered unconstitutional. The law No XX. of 1996. has therefore limited the use of the personal identification number and has decreed the use of separate identifiers for tax and social security purposes.

As a result of this, recently there are multiple sectoral identifiers in use in Hungary (the most important ones are the taxation number, social security number, student number, personal identification number), and the usage of the already existing personal identification number as a general identifier for egovernment purposes is not possible. In fact the personal identification number by the earlier mentioned Constitutional Court decision in practice became rather a sectoral identifier.

At present pupils, students, university students, teachers, pedagogues and professors all have separate identifiers, which make up a large distributed national eIDM system, related to the data registers of the electronic student cards issued by the Minister of Education.

The personal and address data of natural entities which is the central unit of the population register system is managed and operated by the Central Office for Administrative and Electronic Public Service (Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala KEKKH - (http://www.nyilvantarto.hu; available in Hungarian) who also supervises the regional and local databases. KEKKH is responsible for generating the unique personal identification number, and issues the national ID cards which is currently a plastic card without a chip, together with a number of other identification documents which are currently all paper based, and the biometric passport.

According to legislation in force, there are three documents that can be used to prove identity: the ID, the passport and the driver's licence. Thus, it has not been obligatory to carry an ID since 2001, but in practice everybody uses the ID card as an identity provider.

According to Hungarian legislation, the personal identification number linked to the population register can only be used to a limited extent, excluding the incorporation of this identification number in a digital certificate or in any other document, with the exception of the address card (this is a paper based card that is separate from the national ID card but in administrative procedures usually used together with it, and which contains the address data of the citizen and is also issued by the KEKKH).

When a sector introduces a new sectoral identifier a separate official (currently paper based) certificate must be issued in order to inform the citizen about his new sectoral identifier.

An official certificate may only contain 1 sectoral identifier. Thus, public administration in Hungary currently uses the following cards and registers:

- Personal identification document (ID) (mandatory card or a paper booklet from the age of 14) and
- Official personal identification and address certificate (address card with the 11 characters personal identifier)
- Official certificate for verifying social security number – Social security card with a 9 digits Social Security Identification Sign (hereinafter TAJ number)
- APEH tax certificate – Tax card with the tax identification sign (10 digits)
- And the student card should be included in this list, which for those under the age of 14, subject to compulsory schooling, besides providing certain benefits, also serves as proof of identity. The data on the higher education student cards are also stored electronically by the chips on the card.

Ministries and the organs with national jurisdiction co-ordinates the activities of the issuing and of the production of security documents of their subordinate organisations. According the Government resolution No 86 of June 14. 1996 on the rules of the protection of security documents there is a National Visa and Document Committee for a definite range of national documents.

Identification cards required for physical access are widely used both in public administration and business, those however can only be used at the individual premises they were issued for. PKI based authentication is used by a single bank only for the purpose of e-banking, though lately SMS based messaging has been replacing its use.

For eGovernment applications electronic authentication has been provided by the Client Gate of the Government (http://www.magyarorszag.hu/ugyfelkapu). The Client Gate's authentication is based on username and password. In order to obtain a username-password pair the citizen has to appear in one of the more than 200 document offices that cover the country for a face to face identification based on a picture ID (basically the national ID card) Those citizens who have an at least advanced level administrative digital signature certificate can get the username-password by submitting an electronic form to the operator of the Client Gate. In this case the face to face identification of the person happened at the Certification Authority's premises that the Client Gate's operator trusts since the rules of the identification for this case were also set out and are monitored by the administration.

In the course of the registration the authorities verify the data on the photograph bearing ID of the client online in the personal data and address register. The same method is used by the certification authorities that issue digital certificates; however, they also consult the data in the company register, if necessary.

At present further identification (entering of the sectoral identifiers) is required for the use of sectoral and local government applications accessible through the Client Gate since the storage of multiple sectoral identifiers at one place is not allowed by the national data protection legislation. The identification is carried out with the aid of the tax identifier or TAJ number in case of taxation and health services, or in certain cases with the aid of identifiers received in the course of separate

registration procedures. (e.g. labour database, or for local governments.) This in practice means that after entering the username-password when the user gets to the service's screen he/she has to enter his/her sectoral identifier also.

The introduction of an electronic citizens' card has been on the agenda several times since 2001, and has been incorporated into the strategy, but no Government decisions has been taken on the subject after 2002.

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

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

IDM system	Potential user base	Actual penetration	Actual use
National ID card	8 million		No public statistics are available
Driving licence			No public statistics are available
TAJ card	10 million		No public statistics are available
Student card	1,5 million		

In case any of the above mentioned cards gets equipped with a PKI authentication certificate the Client Gate can incorporate them in the system as a hard PKI access card for egovernment services.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

In Hungary, since the beginning of the 90s an organisational unit of the Prime Minister`s Office[3] has been responsible for co-ordinating the utilisation and development of ICT in the central administration (eGovernment), and since 1993 it has taken a leading role in the development of the IT strategy of the ministries. In 2003, the Government adopted the Hungarian Information Society Strategy and within that the eGovernment Strategy and Program. The current version of this strategy is called „e-Government 2005". The Hungarian eGovernment front-end is centralised. The implementator and

[3] 1991 Coordination Office of the Inter-Departmental Committee of Informatics (ITB), 2000 Office of the Government Commissioner for Information and Communication Technology (IKB), 2002 Office of the Government Information Technology and Civil Relations (KITKH) more recently, since 2003 eGovernment Centre (EKK)
http://www.meh.hu/szervezet/hivatalok/ekk/ekk/alap.html

developer of this centralised system called the Central Electronic Service Provisioning System (Központi Elektronikus Szolgáltató Rendszer) is the Prime Minister's Office Electronic Government Centre (EKK). The Central Electronic Service Provisioning System consists of the Electronic Governmental Backbone (Elektronikus Kormányzati Gerinchálózat EKG), the Government Portal[4] and the services accessible through it, the Client Gate, the Office Gate and the Government's Customer Information Centre. The system was developed and is being operated according to the definition of eGovernment services. 27 services in 17 institutions can be accessed by pre-registered users through the Government Portal and Client' Gate. The level of readiness of the services will be 87 percent by 2006. Users can access the services with user name and password and may use an at least advanced level administrative certificate for the registration. More then 520.000 people (68 with qualified electronic signature between them) have registered until April 2007. The most popular services are tax and contributions, admittance to higher education and reservation of time for face-to-face administration procedure in document offices. Users can access the services with user name and password, and may use at least advanced level administrative certificates for registration. The Central Electronic Service Provisioning System also provides the services of some local authorities (and it is possible for entrepreneurs too) based on agreements concluded with the operator of the system.

As a result of the latest development the functionality of the Central Electronic Service Provisioning System has been extended with secure electronic document exchange capability. Citizens after signing on through the Client Gate can send electronic documents to the authorities that connect to the Central Electronic Service Provisioning System through the Office Gate. Part of this development was the creation of a temporary and permanent secure storage area (electronic post box) for the users. When a citizen registers for the username-password or in other words opens it's own client gate a temporary and permanent secure storage are also gets assigned to his/her account.

The Client Gate "knows" only natural persons which means that it stores no role information or other attributes about a citizen. Only the natural identifiers and an e-mail is stored in the system about the user. The natural identifier database of the Client Gate is harmonised with the Register of personal and address data.

For the regional and local institutions of the public administration central co-ordination was carried out by the Ministry of Interior until June 2006 and thereafter by the Ministry of Local Government and Territorial Development[5] with the participation of the Offices of Public Administration of the Capital and the Counties (i.e. 1+19 offices); however, the determining role in e-administration is that of the Electronic Government Centre (EKK) of the Prime Minister`s Office. At the end of 2005 there were 900 different IT projects in progress, supported by different central programs, among which several used or planned to use electronic authentication and electronic signatures as well. Currently, all of these applications are forwarded to the Client Gate.

The different national associations of local governments (7 in all) especially their IT committees support the territorial and regional co-ordination and control. (e.g. National Association of Local Governments[6] (TÖOSZ - Települési Önkormányzatok Országos Szövetsége); National Association of

[4] http://www.magyarorszag.hu/

[5] http://www.bm.hu/web/portal.nsf/index

[6] http://toosz.webalap.hu/

Intelligent Local Governments[7], (ITOSZ - Intelligens Települések Országos Szövetsége); Association of Cities with County Rights[8] (MJVSZ - Megyei Jogú Városok Szövetsége)

MeH ITB (Interdepartmental Committee for IT of the Prime Minister`s Office) took the first significant initiative in 1994 by promoting the use of smart cards as the bases of eID tokens. As a result, the Hungarian Smart Card Forum was established in 1997 in the form of non-profit organisation. In this very year the preparation of the Bill on the use of electronic documents – electronic signature in public administration began, though the Act on electronic signature only came into force on 1st September 2001. Essentially there are only A2A, and B2B electronic signature applications, which, with a few exceptions do not require the use of expensive qualified certificates. On the other hand neither the electronic authentication nor the use of asymmetric encryption/decryption is regulated in the Hungarian legislation. This was one of the reasons why username-password based authentication was first used for the Client Gate[9], though authentication by cellular phone was also investigated.

3.2.2 National eGovernment cooperation and coordination

The Government IT Conciliation Interministerial Committee (KIETB) was the co-ordinating forum of the central bodies from July 2002, its members were the chief executives of the ministries responsible for IT. The parliamentary commissioner for data protection, and a representative of the Hungarian Academy of Sciences, of the Association of IT Entrepreneurs, of the Association of Hungarian Contents Industry, and of the Hungarian Chamber of Trade and Industry taking part in work of the committee. In 2003 the eGovernment Operative Committee (EKOB) was established from the heads of national public administration bodies involved in the operative work. Both committees are chaired by the head of the EKK.

From 2003 the broadest co-ordinating forum of the development of information society in a more general sense was the Interministerial (Inter-Departmental Coordinating) Committee on the Information Society[10] (ITKTB Információs Társadalom Koordinációs Tárcaközi Bizottság) operating under the auspices of the Ministry of Informatics and Communication[11]. This forum coordinated the development of the Hungarian Information Society Strategic and Action Plan[12] (MITS) in 2002-2003. The representatives of territorial and local bodies of public administration also participate in the work of different sub-committees of the ITKTB together with the representatives of the public and private sectors. The most important among these sub-committees from the aspect of eIDM are the E-

[7] http://www.itosz.hu/

[8] http://www.mjvsz.hu/portal/index.aspx?lap=45

[9] CurrentlyRecently there are only 0,017 per cent among the registered users who owns qualified certificate.

[10] Established by government decree No 1214 of 28. December 2002 (1214/2002 (XII.28.) Korm.határozat) - http://english.itktb.hu/engine.aspx?page=itktb_eng

[11] From the 9th of July 2006 the tasks of the Ministry of Informatics and Communications (IHM) with the exception of e-administration were taken over by the Ministry of Economic Affairs and Transport - GKM.

[12] http://english.itktb.hu/resource.aspx?ResourceID=MITSangolPDF

Administration Subcommittee (ELKA)[13] and the Information Systems Security Subcommittee (INBA)[14].

ELKA provided a co-ordinating forum for the dissemination of electronic signature, smart cards, geo-informatics and other sophisticated IT solutions, technologies and devices in public administration. Recommendations were issued in the Framework of Hungarian e-Government Interoperability. (e.g the Recommendation of Smart Card Specifications[15] (HUNEID).) HUNEID is compatible with the European Interoperability Framework (EIF).

e-Szignó/e-Tár (electronic signature and electronic archive) was an important part of the joint sectoral e-Security program in the framework of MITS from 2004. As a result of the program the RootCA for Public Administration Hungary (KGYHSZ) doing only overcertification of commercial certification authorities together with a qualified governmental certification service provider, Security CSP (BHSZ)[16] with time stamp and archiving capabilities were established.

40 percent of the Hungarian population do not live in towns. 81 percent of the 3148 settlements have less than 5000 inhabitants, and in many cases their supply with telecommunication network posed serious problems. This was the reason why during the past years infrastructure development and the spreading of broadband Internet was the most important among the priorities of MITS. The Government approved the MITS in the form of a Governmental decree. (Decree No 1126 of 12 December 2003). Also in 2003 separate e-signature, (smart) e-card, e-security, e-government, e-local government, etc. sub-strategies[17] were developed for MITS. Recently the priority is to achieve broader use of eGovernment services through registration on the Client Gate and to increase the security level of the authentication used at the Client Gate.

The long term goals of the e-signature sub-strategy for the next 10-15 years include infrastructure development according to the CEN, ETSI, IETF standards, the increase of Internet penetration to 70-80 percent, the increase of the use of bank cards, the development of e-Government applications (tax returns, request for documents, company registration and business dealings with the local governments), and increasing the awareness of society regarding the use of e-signatures.

The 3-4 years goals of the strategy were realised: in November 2005 the public administration root CA (KGYHSZ) was set-up, a ministerial advisory committee was created to act as Policy Management Authority (PMA), and through a private initiative MELASZ[18] (Hungarian Electronic Signature Association) was created. In March 2006 NHH (National Communications Authority) registered the qualified authentication service provider BHSZ, which however, according to the

[13] http://english.itktb.hu/engine.aspx?page=elka_eng

[14] http://english.itktb.hu/engine.aspx?page=inba_eng

[15] http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=986&t=stored (in Hungarian only)

[16] http://www.kgyhsz.gov.hu and http://www.bhsz.gov.hu (later is a common portal for all CSP`s involved in the Hungarian Public Administration PKI - MKPKI.)

[17] http://www.itktb.hu/engine.aspx?page=dokumentumtar&docstorefolder=45

[18] http://www.melasz.hu

Government decree only provides services to high ranking government and security services officers, besides providing time stamp and electronic archiving services. The independent governmental CSP of advanced and qualified electronic signature for the public administration however was not implemented, since on the basis of the legislation published in September 2005 and the compulsory public procurement norms commercial CSPs overcertifiied with the earlier mentioned national root CA (KGYHSZ) can provide certificates for public administration. The Act XXXV of 2001 on electronic signature was reviewed in 2004 and several new laws were published. Also the conditions for e-administration were regulated.

The tasks defined in the smart card strategy covered 3-4 years. The HUNEID standard for intelligent cards was published on the basis of CEN CWA 14890, and the Java based sample implementation corresponding to the file structure and the card interface specification were also published. Besides the eGovernment interoperability framework[19], also the guide for eGovernment technical standards was created. In 2006 the first HUNEID compatible application product (professional medical card, health card pilot) appeared. The introduction of public servant card or citizen card however, were not on the agenda.

3.2.3 Traditional identity resources

Act XXXIII. of 1894 made state registration mandatory in Hungary. Act XXVIII of 1879 already meant the beginning of the legal regulation of population registration on the basis of the register of birth, marriages and deaths. It was this act that ordered the obligation of registering one's address (back then of the registering of home) and in connection to that the registration of changes in address, in the framework of the state police.

Before the end of World War II the obligation to register one's address - which by that time was distinguished as being that of either temporary of permanent residence - was regulated by several decrees, the most comprehensive one being Decree of the Minister of Interior No. 380.000/1941. BM. During the world war the larger part of the address register was destroyed. The registration means the issuing some kind of identity documents, which had an important meaning for the civil population and the occupational armies in the war times and after.

After 1945 the obligation to register was initially regulated by decree of the Minister of Interior. Later the citizenship Act LX of 1948 was enacted to resolve the problems of an incomplete, inexact, and not up to date population register.

A new type, personal identification document have been compulsory in Hungary since 1954. The police issued the very detailed document as a hard covered paper booklet, with many pages containing not only the personal data and addresses (permanent and temporary) but all other information. (data of spouse and children, place of work, profession, etc.). The personal identification number was given in it since 1986. In the nineties the content decreased drastically, the hardcover changed to soft with the coat of arms of the Hungarian Republic and the Central Office would be responsible for the issuing instead of police. From the 1st of September 1996 the official personal identification document contained:

[19] http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=800&t=stored

- family name and given name;
- maiden's name, (according to the Act No. XLV. of 2002 it is the name of birth in the followings);
- place and date of birth;
- mother's name;
- personal identifier;
- address, dwelling address time of validity;
- document identifier.

Nowadays the personal identity card contains the following data: last name, first name(s), last name and first name(s) when the bearer was born, date of birth, place of birth, nationality, mother's name, gender, picture of the bearer, handwritten signature of the bearer, number of the identity document and validity period of the card, date of issuance of the card, the code of the issuer state, Hungary and the name of the issuer authority. Any people included by the law in the population register from the age of 14 may apply for the card, but it is not compulsory.

There is a separate document containing the personal identifier and the address.

The validity period depends on the age of the bearer. Under the age of 20, the validity period is 6 years; above it becomes 10 years, or unlimited above the age of 70.

During the data processing of the census of 1960 the public administration in Hungary was increasingly faced with the problem of the registration systems. The registration systems being difficult to manage, their handling became more and more complex. At the same time computerised population registers provided the basis of registers of the government in several western European countries. A law of 1974 on the Creation of the Population Register yielded the legal basis for today's registers.

The decision of the Council of Ministers No 2001 of 1970 MT determined the purpose of the new population register. The development of a new computerised population register began on the basis of the Finnish experiences. The model of the population register and the system of the personal identification number (nowadays personal identifier) were elaborated during the period of 1973-74. A census was carried out between January 2 and 15, 1975, and parallel to that the State Population Registration Office began its operations on July 1 1974.

The 11 digit personal identification number is a semantic number. The first digit indicates the gender and the time period of birth or the foreign citizenship and the next six the year, month and day of birth. The usage of personal identification number on any public documents by itself harmed the privacy of some people. This was the reason for it to be contested at the Constitutional Court in 1990.

The aim, task and regulations of the state register has been determined through the years by legal regulation of various levels during the period of the 1970s and 80s according the political course of the soviet model. The unrestricted, general and unified use of the personal identification number according that regulations violated the Constitution. The resolution No 15 of 1991. of the Court of Constitution annulated the laws on the population register: Decree with the force of act No. 10 of 1986

of the Council of Ministers and the decrees for its implementation No 25 of July 8. 1986 and No 102 of July 3. 1990 of the Council of Ministers.

The current system was constructed and - in harmony with the provisions on the protection of personal data in the Constitution and according to the data protection Act LXIII. of 1992 - on the basis of Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens. The Act XX of 1996 very strictly limited the use of the identification codes. The use of the personal identification number is allowed mainly in the information systems of the KEKKH (and recently in the cadastre). Temporary connection codes are used for updating other registers, e.g. tax or social security on the basis of the population register.

3.2.3.1 The Administrative System of Registration

Act LXVI of 1992 on the Register of Personal Data and Addresses of Citizens indicated that the aim of maintaining the register of personal data and addresses is to enable citizens to properly identify their person amongst themselves in their legal relations to each other, and also enable the public and justice administration, local governments as well or other organisations to request data from the register- within the framework of the legal provisions.

The scope of the personal data and address register includes that data of:

- Hungarian citizens living within Hungary;
- Hungarian citizens living abroad and requesting to be included in the register;
- foreigners who immigrated to Hungary and are acknowledged as refugees

for the following data according to the authorisation granted by the Act:

- name;
- Hungarian or foreigner citizenship, immigrant, refugee status or EEC permit;
- gender;
- place and time of birth;
- mother's name;
- personal identifier;
- time and place of death;
- address;
- limitation or prohibition of data services based on this data;
- label of permanent data services based on this data;
- marital status and place of marriage;
- portrait photograph, signature;
- identification numbers of the personal identification document (personal card) and of the document on the personal identifier and on address (address card)

The system of registration operates on three levels. KEKKH is the first- and second level authority with regard to personal data and address registration.

At the local level - at the local government of the settlement or of the small territorial district – it is the task of the notary of local government or of the district centre:

- to keep the register either manually, or with the aid of computer software;
- to provide data with the conditions as determined by the Act; and
- to forward data and data modifications included in the register to the central register.

At the regional, county as well as the metropolitan level the tasks of the Head of the Office of the Public Administration are:

- to participate in the formulation and maintaining of the maintenance link between the local and central register;
- to operate the computerised register in the counties and the capital city;
- to authorise the providing of data from the register according to the conditions prescribed by the Act; and
- to oversee the direction of the local register.

At the central level the tasks of the President of KEKKH are:

- to generate the personal identifier (before January 1, 1997 the personal identification code, earlier the personal number), to ensure their issuing, modification and revocation through local authorities, registrars, and foreign missions;
- to operate the central computer system of the register, as well as the registry of personal identification cards, and that of the central document bank;
- to carry out the data service from the central register according to the conditions determined by the Act;
- to manage and control the professional aspects of the operation of the register at the local and county levels;
- to manage the Central Document Office as part of the KEKKH and to control more than 250 Document Offices in the country. (The Central Document Office of the KEKKH issues the personal identification cards and most of the identification documents as well).

The protection of personal data is ensured at each of the three levels.

Data services (see below, section C.3.4.) using information contained in the register may only be implemented after the duly diligent examination of the aim of use and legal basis for the processing as indicated by the requestor. According to the provisions of the Act, a separate register is to be maintained in connection with the data service, and if necessary those involved must be notified of the time and the aim of the processing, and to whom data was given to from the register. Citizens have the right to limit data service from his or her data. In such cases it is only data services for the purpose of the operation of organisations authorised by the Act that may be carried out.

3.2.3.2 The IT System of the Register

The IT system of the personal data and address register - similarly to the administrative structure - operates at three levels.

At the **local** level - at the local-governments or at the territorial district centres (currently at more than 2700 locations) the registration and service system containing the data of citizens residing or temporarily residing within their jurisdictional area is being operated. The local level is connected to the county registers on the nationwide data processing network and at more than 270 document offices at this time.

The **county** level ensures the connection between the local and central level, provides an opportunity for the preparation of county level services. The system operated here is connected on the nationwide data processing network to the central system.

The **central** register contains the personal data of every person falling under the jurisdiction of the register.

The central level operates:

- the service sub-system, which gives an opportunity for providing direct and indirect (batch) services;
- the personal identification card register, which contains the photograph and signature of the citizens, as well as data regarding these documents; and
- the central document bank.

The IT system of the personal data and address register is comprised of two main parts: the personal and the address data.

Data stored with regard to persons includes:

- personal identifier;
- name data;
- birth and death related data;
- gender;
- citizenship;
- status indication (refugee, Hungarian national living abroad, or in Hungary);
- indication of limitation of data-release;
- as well as other technical data.

The maintenance of the central register with the changes arriving from data-sources is carried out on a regular weekly basis. The input of data and its preliminary processing takes place at the local level already, and the changes are communicated from the territorial level through the network to the KEKKH. Feedback and notices back to the territorial or local level travel the same way each week.

Among the three levels of personal data and address registration it is the central that is to be considered authentic, data contained in the systems operated at the other levels only become authenticated following central maintenance, after the updates notified from the central level have been included in them.

Data stored with regards to addresses includes the county name, name of settlement, data of public premises (name, type i.e. street, place, etc., postal code), HoBStaFlAp data (**Ho**use number,

Building, **Sta**irway block, **Fl**oor, **Ap**artment - „HÉLSZA" is the Hungarian equivalent acronym), and district data.

The address register of the central system contains historical data also. The maintenance of the system, just as in the case of personal data, is carried out on a regular weekly rotation, on the basis of the local data received at the centre through the territorial level.

3.2.3.3 Personal Identification Card Register, Central Document Bank

The KEKKH operates the Central Document Bank of the personal data and address register, which contains the documentation created during the registration procedure, related to inclusion in the register, deletion from it, to the limitation of data services, the modification and correction of data. The central document bank does not, however, contain the basic register documents (birth, marriage and death certificates). These are stored by the Registrar competent according to the place of the event.

Besides the documents containing personal data the document bank also accommodates the storage of instruments regarding territorial and public administrative grouping, and address modification measures.

The Central Document Bank contains the personal identification card datasheets and photographs as of June 1, 1993, and also the address registration datasheets.

The task of the Document Bank is to organise and store the documents received by it, and the provision of data from them upon demand.

3.2.3.4 Data Services

The personal data and address register has become an integral part of the major information systems of both public administration and the judicial branch, it is an effective means of decreasing the burden of citizens related to administrative issues and also of vindicating their rights, as well as fulfilling their obligations.

The organs of the register may provide data on condition of that proof is provided of the aim and legal basis of the usage of such data.

In order to facilitate the legal link between data managements of different purposes, temporary series of numbers, link codes are generated to repeatedly request and supply regular data on the same private entity, and to update the records relating to the entity requesting these data. Different link codes must be generated for the same private entity by each entity requesting data. The link code can only be used for the purpose it was generated for; after the purpose was completed this code must be deleted from the records of both the entity requesting and supplying the data. The link code

can only be managed and transmitted by the body responsible for the register and the entity requesting the data.

The body responsible for the management of personal data and address register must supply regularly data – using the link code – to the following bodies:

- tax authorities;
- social security, for the health fund register;
- social security, for the pension fund register;
- the State Supervision of Financial Organisations on the death of persons in the Central Register of Funds.

The body responsible for the management of personal data and address register must regularly supply data – using the personal identifier – to the following bodies:

- the defence administration;
- the bodies responsible for the control of aliens, on the immigrated and settled citizens;
- *the bodies responsible for the registration of penalties;*
- the bodies responsible for managing the road traffic register.

The KEKKH – along with the local and territorial organs of the register – provides 40 million data services yearly. It satisfies the data demand of both the tax authorities and social security bodies, provides direct services to organisations carrying out judicial and criminal tasks.

The Central Customer Service Branch provides services to any person or entity, or organisations without legal entity, with strict adherence to the provisions determined by law.

The Act also takes the demands of science and a market economy into consideration, making it possible to provide name and address data for scientific research, market research, opinion polling and direct marketing purposes. Naturally citizens taking advantage of their right to limit the provision of their data are not included in such services.

The Office publishes the statistically processed personal and address data contained in the register every year. Apart from that it also satisfies demands for the preparation special statistics according to specific areas and age groups, as well as genders and family status.

The Central Document Bank regularly provides data to judiciary and criminal organs. The data of approximately 280 000 citizens is given out every year on the basis of the stored documents.

In justified cases the document bank provides information on the loss, stealing or destruction of the personal identification card upon the request of citizens, entities, and organisations without legal entity.

The data service for organisations fulfilling public tasks is free of charge, in other cases applicants have to pay a fee for the service, to an extent determined by the Act.

The national register of companies and the included information service is an old application of the Ministry of Justice and Law Enforcement. Since the 90s the information service is accessible online. The regular amendments of the act on the registration of firms allowed for its modernisation. Due to the Act LXXXI. of 2003, the electronic procedures of firm registration came into reality step by step in the period of 2005-2006. Nowadays the Company Register based on a distributed database resides at 20 District Courts of Hungary, which accept paper based and/or digitally signed electronic application documents for registering (change management), deposition of annual accounts, and providing information by electronic means. The registration can be initialised by the company owner, by a lawyer or by a public notary. The application provides public online (internet) access to the Company Register. It supports automated distribution and conversion of company data for registered users/organisations. The abstract on company data, the copy or the company certificate issued by the Company Information Service are authentic public documents in paper or electronic form.

The traditional identity infrastructure can be said to consist of distributed locally maintained paper and electronic registers for natural persons, and maintained on county level for legal persons, and a group of personal identification documents in bankcard format to natural persons.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

3.3.1.1 The Client Gate

eGovernment services can be accessed using the Client Gate, which is a part of the Central Electronic Service Provisioning System managed and operated by the Electronic Government Centre (EKK) of the Prime Minister's Office.

The Client Gate functions as the identification gateway of the administration. Except for local authorities' eGovernment services every eGovernment service is obligatorily accessible through the Client Gate. But most of the local authorities services are also available through the gateway.

The user provides his or her user name and password in the login process, and the Client Gate sends to the application (the service chosen by the citizen) the name, the e-mail address, a qualifier related to the credentials and roles of the user, and a temporary transaction code (artifact) from the registration register of the Central Electronic Service Provisioning System. The service that the citizen accesses through the Client Gate may ask for an identifier, e.g. the tax number or TAJ. If necessary the Client Gate provides a service called (re)identification in order to allow the service providers to verify the natural identifiers of the citizen accessing their service. The process is detailed later.

The rules of electronic administration are contained in articles 160- 162. § of the Act No. CXL. of 2004 (hereafter Ket). According to those rules, if the client has at least advanced level administrative electronic signature he/she can submit his/her application on the Central Electronic Service

Provisioning System or directly to the authorities otherwise (meaning that he/she has no digital PKI certificate) he/she is obliged to use the Client Gate for service access. With the credentials obtained in the course of the preliminary registration the client creates his/her own client gate in the CESPS. Since in practice very few people have digital signature certificates every citizen uses eGovernment service through the Client Gate.

Registration can be carried out by a face-to-face identification in one of the document offices, or via an at least advanced level administrative certificate where the registration was carried out by the registration authority of the issuing CSP. The clients only use their name and e-mail address in the Client Gate, and in their applications they only have to give their personal data to the extent prescribed by the legislation for their specific case application; these personal data cannot be used by the central system for personal identification.

When a person opens a client gate (registers for a username-password) he/she also receives a secure storage area (electronic post box) which has a temporary and a permanent storage component.

3.3.1.2 *(Re)identification* (verification of personal data)

The digital certificates mustn't contain either the personal identification number or the natural identifiers except the name and the e-mail address of the certificate holder in Hungary. The Act No. CXL. of 2004 on the general rules of public administrative procedures and services (hereafter Ket) has introduced the institution of (re)identification to solve the problem of data protection arising in connection with the on-line identification of persons. The method of (re)identification provides the result of identification without transfer of personal data stored at the Client Gate or at Certification Service Provider (CSP). Basically in a single-sign-on system if the user signs on his attributes are transferred for the service providers from the identity provider, which in our case is the Client Gate; but for data protection reasons this is not allowed in Hungary. Only the name and the e-mail address of the user gets automatically transferred to the service provider after sign on. The other attributes (the natural identifiers) of the user can be discovered only by the process of reidentification.

When the user signs on, only his name and e-mail address is transferred to the service provider. In case the service provider wants to know the natural identifiers of the user for identification purposes it has to find it out for itself first. It can do so either by asking the user to tell it directly (entering it into an electronic form), or if the service provider already has a database (usually in this database the natural identifiers and a sectoral identifier of the person is stored together) then by retrieving it from there by asking the user to enter his/her sectoral identifier while using the service. After the service provider manages to acquire the natural identifiers of the user in any of the ways mentioned earlier, based on that it can ask the Client Gate to verify that data.

For the verification the service provider sends the earlier mentioned transaction code (which functions like a temporary connection identifier) to the Client Gate (this is the data from which the Client Gate knows which logged on users' reidentification is going to happen; the transaction code was earlier issued by the Client Gate and sent to the service provider and is valid for one connection only) and the natural identifiers. If the natural identifiers sent to the Client Gate are the same as those which are registered in the Client Gate's database about the person who logged on and got the given

transaction code, then the reidentification is successful and the person's natural identifiers are verified.

The same methodology is used in case of PKI based identification, but in that case the user's digital certificate and natural identifiers are used and the reidentification is done by the certification authority that issued the certificate.

By law if a certification authority wants to issue certificates for administrative usage it has to provide reidentification services for public authorities. This is one of the extra features of an administrative certificate.

According to point (2) Article 160. § of Ket : „For the purposes of identification the authorities may verify the validity of the signature and the natural identifiers of the signer at the CSP involved in the form of reidentification, this however shall not affect the obligation of supplying the personal data provided for by the legislation based on which the specific procedure would be carried out. In the case of the use of electronic signatures for public administration purposes the CSP upon request of the authority responsible for that specific business will carry out the reidentification and will inform the initiator of the request about the results of the validation."

In case of PKI based identification in the course of reidentification the authority verifies that the data legally available on the client and the personal identity data actually collected by the CSP when issuing the certificate used are identical. The application, on the basis of the available personal identification data and the digital certificate of the signature submits a request to the CSP for reidentification.

The request should contain at least the following data:

- Name or birthname
  - Family name
  - First given name
- Mother's name of birth
  - Family name
  - First given name
- Place of birth
- Name of the settlement of birth
- Date of birth

The request will be signed electronically by the requesting authority. The Client Gate or the CSP will return the result of the verification to the requesting authority (application) in the form of a YES/NO message. The response will be signed by the CSP with its own signature.

The Act CXL. of 2004 on the general rules of public administrative procedures and services defined the Client Gate as part of the System of Central Electronic Services. The Electronic Government Centre (EKK) of the Prime Minister's Office manage and operate the System of Central Electronic Services according the point (2) of government decision No 1044 of 11 May 2005). Government

decree 193 of 22. September 2005 on the detailed rules of electronic administration regulates the process of services.

The Client Gate ensures access to the eGovernment service providers for the user who preliminary registered themselves. The registration should be made on the Client Gate and following that with a personal, face to face identification and with personal identity document, passport or driving licence at a Document Office or on the other hand with an at least advanced level administrative electronic signature (see in the next paragraph) of the declaration attached to the registration form. In the latter case, 24 hours is required for the verification of the certificate.

The Client Gate accepts only the certificates of the CSP where the Registration Authority provides the face to face identification. This is required for qualified certificates and in some cases for advanced certificates. The advanced certificates issued according to Government decree No. 194. of 22 September 2005. (i.e. with face to face personal identification) are therefore also acceptable.

In case of a foreigner the registration process is similar. A person who is not a resident or who doesn't have residence permission, should use his or her passport for the identification in the Document Office.

After a successful registration, the Client Gate sends an e-mail to the applicant's address with a one time password which should be changed by the user. Normally the client can log in with his or her user name and password at the Client Gate, however the desired service may ask for some stronger authentication.

The Central Electronic Service Provisioning System as a collection of information systems and services provides the infrastructure, the communication platform of services, the authentication needed for the access of services, and the information service for the administrative deals and for the technical questions:

- The Electronic Governmental Backbone (EKG) provides the infrastructure (The EKG connects 740 sites of organisations and has been serving about 58.000 users of the central public administration in May 2006);
- the Government Portal provides the possibility of appearance for the services. The portal not only links the eGovernment services of different sectors but collects information from the 46 most important governmental websites, however other services can operate their own portal.
- the Client Gate provides the authentication needed for the users of services (33 governmental organisations provide the services)
- The Office Gate is the point through which public authorities connect to the system and receive the electronic documents sent to them by the citizens.
- the Government's Customer Information Centre serves as the helpdesk and call centre. (There are 264 information and/or searchable services, more than 2000 downloadable forms and more than 1000 descriptions of administrative cases).

The start-up of the first Government Portal was in December 2001. The user at that time could search in three databases (in the register of companies, in the register of vehicles and in the register of immovables). The 20 basic eGovernment services according the eEurope Common List of Basic Public Services (which are 27 in Hungary) yield 80 per cent of all administrative cases. There are about 400 other related cases too, which can be handled. Using the Client Gate the customer can

start more than 80 cases at the Virtual Document Office or settle the time of a personal administration for 86 cases in any of the about 270 Document Offices.

Since 1 April 2005 it is possible to initiate or handle by electronic means, those administrative processes, which require personal identification; however an eID card is not yet implemented in Hungary. The system satisfies even the strongest requirements of data protection. Recently the system provides access to the tax and contribution declaration services of the Tax and Financial Control Administration (APEH), to the services of Document Offices, to the services of the Company Information Service, to the services of the two Social Security Founds (OEP and ONyF), to the services of the Public Employment Service, to the services of the National Higher Education Information Centre, and to the services of more and more local governments.

The Central Electronic Service Provisioning system provides the possibility of secure document exchange between citizens/businesses and the public administration through a secure electronic document transmission system. The number of visitors had risen above 3 millions on the Client Gate due to the possibility of electronic submission of the application forms for higher education and due to the obligatory electronic submission of tax declarations of the enterprises at the beginning of the year 2006. The new system received and confirmed 500.000 tax declarations in one month at the time of the ultimate deadline for the first submission in May 2006, and there were 2,4 million at next time in February 2007. There were above 20 million visitors in the period of January-February 2007. The number of registered users was about 520.000 in that time.

The registration process of the Client Gate

All entities resident according to law can be registered as user at the Client Gate. A temporary registration can be made on-line on the Governmental Portal (http://www.magyarorszag.hu/ugyfelkapu/regisztracio/ideiglenes). The following data should be sent or signed with qualified electronic signature.

- **Natural personal identifiers**
  - Used name: family name, first name
  - Name in the time of birth: family name, first name
  - Gender
  - Place of birth
  - Date of birth
  - Mother's name
  - Citizenship

- **Data for the Client Gate**
  - User's name
  - E-mail address
  - Time of validity

For the electronic signature the SDX Browser Edition eSignature Application (XML type of eGroup) can be downloaded during the registration process. The signed application will be usable after a 24 hours retention period.

In case of registration without electronic signature the temporary registration is valid for 30 days. It bears only limited rights, but the user may ask for an appointment at the nearest Document Office for the face to face registration in that 30 days time. The registration data will be verified with an identification document (personal identification card, driving license or passport with address card) in the national registers of the KEKKH.

The registration is valid for 5 years. The user should have an e-mail box for that time.

3.3.1.3 The personal identification document

The definition of personal identification document

The personal identification document (ID) is an official certificate issued on the basis of the written statement of the citizen, the birth certificate and the data of the personal data and address register – in the case of foreign citizens also the passport of the citizen and an authentic document proving the address of his/her residence in Hungary – which verifies the identity and data of the citizen established by the legislation in an authentic manner. The personal identification can first be issued when the citizen reaches the age of 14.

There are three types of valid personal identification documents in the Republic of Hungary. Since the 1st of January 2000, those applying for identification documents for the first time were issued plastic (polycarbonate) cards containing the personal data, photograph and signature, but if the old booklet type documents get lost, expire or are destroyed, they are also changed for this type of documents. The two older booklet type documents (hard cover with the coat of arms of the people's republic and soft cover with the coat of arms of the republic) continue to be valid and they don't need to be replaced until they expire.

The personal identification document contains the name, name of birth, place of birth, date of birth, nationality, mother's name, sex, photograph and signature of the bearer or the signature of the legal representative if the bearer is placed into custody limiting or excluding legal capacity; and also the identification number of the personal identification document, the validity period, the date of issuance, the code of the issuer, Hungarian State and the name of the issuing authority.

The definition of address document

The purpose of the address document/card is to inform the citizen about his or her personal identifier and about his or her declared address in the interest of authentic certification in case of doing his or her duty prescribed by the law (e.g. at the time of elections).

The content of the official document for the certification of the personal identifier: family and given name; name of birth; place and time of birth; mother's name of birth; personal identifier; address, and address time of validity; and the document identifier.

Documents suitable to prove identity

Besides the personal identification document, the citizen can use all official documents (passport together with the address card, card type drivers' license), which contain the bearer's name, place of birth, date of birth, nationality, photograph and the bearer's signature.

There isn't any prescription for the electronic authentication and/or identification in the Hungarian law. However, the certification services provider can issue special certificates for authentication purposes This possibility seems to be rather expensive and not used in practice.

The authorities e.g. at the document offices, police etc. may identify a person with identification document on line in the population register.

3.3.1.4 The Social security card with the 9 digits Social Security Identification Sign (hereinafter TAJ number)

The TAJ number is a personal identifier issued to every Hungarian citizen after birth, normally for life. The National Health Found generates the TAJ number.

Foreign citizens can get a TAJ number in case of an insurance relationship or agreement for health services.

The official document of the TAJ - the TAJ card (Certificate of entitlement for health services) – is needed for social services.

The official TAJ number document is issued and delivered to the bearer by the National Health Found. The official document contains:

- family name and given name;
- date of birth;
- TAJ number; and
- the seal of the issuing body and the signature of the issuer.

The endeavour for the use of smart cards (ICC) has been present at the earliest in the Hungarian health sector. During the years a number of projects and experiments have been carried out. The Hungarian Chamber of Doctors (Magyar Orvosi Kamara MOK) issued the first multi-functional, professional doctors' card already equipped with PKI capabilities in conjunction with a bank. By 2006 the second generation of professional doctors' card was also ready.

The compulsory introduction of the European Health Insurance Card by 2008 provided an impetus for the Health Fund, to extend the application of their PKI based identification and signature applications developed for their internal use and for health service providers by the introduction of multi-functional cards to replace the TAJ cards (social security identification cards). However, these plans are not being implemented in 2007 either, due to the shortage in public funds. At the end of September 2006, a three months pilot project was completed successfully.

The new, multi-functional experimental card used in the project contained all the collective data of the TAJ card, the European Health Insurance Card, the Pensions Card and the data required to access

the Client Gate (digital PKI certificates on the long term), thus this card is suitable for the verification of eligibility both in Hungary and the EU member states.

The assets utilised allow the electronic identification of the insured persons arriving from the EU countries with similar cards.

The experiment was carried out in three of the western counties of Hungary, with the participation of 9 family doctors, 12 workstations of 4 hospitals and the 16 thousand potential patients covered by them as well as the pharmacies operating in their area. The doctors used their professional cards, and 11.370 insured people received insurance cards. The insured people participating in the experiment could manage the electronic transactions related to E-receipts and E-admittances, E-travel vouchers. The participating doctors wrote out close to 3.000 prescriptions during the three months period, and registered more then 2.000 patient admittances and releases.

The characteristics of the health card:

Only the keys and certificates were stored electronically on the card as a result of the several years studies carried out prior to the pilot project

The front surface of the card with chip contact contains the data of the Hungarian official certificate; the back of the card contains the data of the European Health Insurance Card. However, for the purpose of electronic identification, the card does not contain only the TAJ data and the certificates required to allow data management. Access through the Client Gate and access to other eGov applications was also possible, as digital PKI certificates and electronic purses, etc. too could be installed on the card.

MOK (Hungarian Chamber of Doctors) issues a similar, but higher capacity SSCD card, on which the certificate required for qualified electronic signature can be installed.

3.3.1.5 Other systems

The students' card

In May 1997 the Ministry of Education issued an invitation to tender for the production of credit card shaped centrally managed student card, uniform throughout the country. On the basis of the one million applications forms submitted by July 1998, by December the winner produced the cards and in the course of 1999 all primary, secondary and higher education students were supplied with student cards.

The pilot run of the student card, which provided electronic identification and aid in the management of business transaction started at the universities of Pécs. 15 thousand higher education cards with microprocessors were issued for the project for the scholar year of 1997/98.

The parts of the legislation on education relating to the central registers and information systems provide the statutory background for the system. Together and supplementing each other, the central register on natural entities and the electronic identification and authentication solutions can provide a suitable basis for the educational administration and for the value added services. According to Government decree 17/2005. (II.8.) on the students' card – currently in force – in order to accommodate electronic transactions about 5.000 public education institutions and 66 higher education institutions needed to set-up infrastructure suitable to accept cards.

The students' card is an ID1 sized plastic card containing the photograph, signature, family and given name, place and date of birth, address or address of dwelling and nationality of the bearer, as well as the unique identifier of the card, the data of the educational institution(s), a small figure, so called pictogram representing type of enrolment (full-time, night course, course by correspondence or distance training), the day of issue, the 10 digits unique identifier of the card and the student identification number established by the legislation. These data are entered into the card by laser engraving technology.

The permanent, higher education student card is also equipped with an electronic circuit, a chip.

The higher education students' card was the first – and up to now the only – document used for electronic identification and the certification of entitlements, listed in the attachment of Government decree 86/1996. (VI. 14.) on the protection of security documents as a document of category „B". Certain main components of the category „B" security documents must be protected against falsification with suitable chemical, technical, technological and administrative methods.

The students' cards are issued by the Ministry of Education and the practical activities relating to the use of the chips on the cards and the technology transfer tasks are carried out by its background institution, Diák-Bónusz Kht.

The Hungarian students' card can be used for identification, for the verification of the legal status and also to make use of travel, cultural and commercial benefits.

About 1.6 million cards are used in public education and close to 400 thousand in higher education; the number of cards replaced and issued every year is around 300 thousand. About 5-8 thousand senior pedagogues and university professors have PKI based eID tokens for identification and electronic signature purposes. The cards, supplemented with non-contact module stickers are becoming increasingly popular for physical access control

The establishment of an infrastructure for the acceptance of cards, and the centralisation of electronic transaction management allow the institutions of public and higher education to make use of the central authentication and electronic signature infrastructure – which currently operates within a restricted circle – to provide all official documents, reports, applications with electronic signatures.

The student certificate is issued by the Minister of Education. Visually, the permanent students' certificates contains:

- a photograph of the student;

- the student's family and given name, place and date of birth, address, nationality, and signature of the bearer (or the signature of the legal representative if the student cannot write or the student has been placed into custody limiting or excluding capacity);
- the name and address (settlement) of the institution(s) where the bearer is a student. The location – in conformity with the official list of institutions published by the issuer – where the training actually takes place serves as the address of the institution. In the case of students who are Hungarian nationals, and are studying in foreign institutions the legend „studying in foreign institution";
- the indication of the branch (with a pictogram);
- the day of issuance;
- data indicating validity [for students over the age of compulsory schooling according to 6. § (3) of the law on public education, and for higher education students a validation sticker];
- the 10 digit unique identifier of the students' card;
- the student's identification number defined in the law on public administration and the law on higher education

On the basis of the requirements listed for the higher education cards in the original tender, the Gemplus MPCOS-EMV 8K type PVC card was chosen with the following characteristics:

- 1 Kbyte application memory, which provides sufficient capacity to store the necessary data and to run different applications.
- The files can be protected by several secret codes, and separate read-write rights can be allocated to each file.
- The financial functions are managed by the microprocessor on the card, and are protected by 3DES based encrypting.
- A Security Access Module was developed for the card, making the use completely secure.
- In the course of production each card is given a unique identifier.
- The material of the card is suitable for personalisation through laser engraving.

The parts of the chip card's memory:

- Bearer data (name, date of birth, etc.).
- Electronic stamp application, for the identification of the institution and certification of the student status.
- Electronic purse for the dedicated government non-cash means of payment (e.g. subsidy for study books).
- Two more electronic purses for general non-cash payment and the collection of regular customer bonus points.
- Free memory space for data storage.
- The serial number, unique identifier and validity date of the card.

The data stored in the memory must be suitably protected. Different access rights can be allocated to the different type of data and applications, this way, only those with access rights to a specific set of data can write, read or delete them (that is, resource management can be set-up).

There were attempts to update the technology of the students' card, however, the process of public procurement was not finalised.

Applicable legislation:

- Act LXXIX of 1993 on public education (hereinafter law on public education) regarding the ten digits pedagogue and student identification number.
- Act LXXX of 1993 on higher education (hereinafter law on higher education) regarding the higher education student identification number.
- Government decree 86/1996. (VI. 14.) on the protection of security documents
- Government decree 269/2000. (XII. 26.) on the general rules for the admission procedures to institutions of higher education.
- Act LXII of 2001 on the Hungarians living in neighbouring countries (popularly known as the „status law").
- Government decree 17/2005. (II. 8.) on the students' card currently in force for the execution of the relevant sections of the laws on public education and higher education (The repealed decrees in their historical order are: Government decree 20/1997. (II.13.). Government decree 30/1999. (II.15.) on the students' card, decree of the Minister of Education 15/1999. (III.24.) OM on the production, issuance and registration of students' cards, Government decree 310/2004. (XI.13.)).

APEH tax certificate

There is also a tax card with the tax identification number (10 digits). According to the Act No XX of 1996, the state tax authority (APEH) should issue the tax card for every taxpayer for the first time on September 30 1996.

The data (family and given name, mother's name, place and date of birth) for the document and the registry of APEH are taken over from the personal data and address register of citizens. The tax card is valid only with authentic personal identification.

The tax certificate contains:

- family name and given name;
- mother's name;
- place and date of birth;
- tax identification sign;
- date of issuance.

3.3.1.6 Authentication policies

There is no official authentication policy in Hungary that defines a strict hierarchy of the different authentication systems in use. However, there are some documents preparing the decision making

connected with a four level authentication[20]. The principle does not differ basically from internationally accepted practices.

The public services of eGovernment can be used without authentication.

The usage of username and password are general in most of the systems, however in some cases strong authentication is compulsory.

The soft and hard certificates are used rarely for authentication. Use of one time passwords (OTP) is spreading (with generators or SMS).

The public administration requires a preliminary face to face registration. Any application of the personal identifier is forbidden for such purposes; however the tax number or the TAJ can be applied in their special systems.

3.3.2 Legal framework

It should be noted that Hungary has no specific regulations with regard to the process of authentication in general. The e-Signatures law No XXXV of 2001 transposes the provisions of the e-Signatures Directive. It is well known that the Directive does not apply to authentication as such.

The first regulation on country-wide registration of personal data was found in the Law No. XXVI of 1545 concerning the men of military age. Recently the identification is based on the registration of birth, marriage and death. The state register is mandatory since the Act XXXIII of 1894, and it is managed by the registrar in the communes. The current legislation in force is the following:

- Act IV of 1952 on marriage, family and guardianship; and the
- decree with the force of law No. 17 of 1982 of the Council of Ministers on the registers, on the procedure of marriage and on the bearing of names

  The new definitions of the “name of birth” and of the “name of marriage” amended slightly of the legal framework and the content of the identification documents since 2004.
- Act XXVIII of 1879 ordered the obligation of registering the address of the population and in connection to that the registration of changes in address, in the framework of the state police. Various forms of legislation of the Minister of Interior regulated the registration and the identification documents until the first personal identification document with photograph was issued in 1954.
- The decision of the Council of Ministers No 2001 of 1970 MT laid down the legal basis of the country-wide computerized population register. The legislation of the following years on the population register and on the personal identification number was annulated in 1991. (Decree with the force of act No. 10 of 1986 of the Council of Ministers and the decrees No 25 of July 8. 1986 and No 102 of July 3. 1990 of the Council of Ministers.)

[20] E.g.: IHM 7147/2003 Az elektronikus aláírás közigazgatási alkalmazásának programja December 2003.

Currently, the legal framework for the population register and for the identification is the:

- Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens, which follows the regulations of
- Act LXIII of 1992 on the protection of personal data and publicity of data of general interest

The main rules on the use of identifiers are laid down in:

- Act XX of 1996 on the methods of identification replacing the personal identification sign and on the use of identification codes, with
- Act LXVI of 1996 on the amendment of acts related to the use of the tax identification sign, of the Social Security Identification Sign and of the personal identifier

The main restrictions regarding the eID tokens are formulated in these acts. (E.g. the usage of identification number of the population register as a unique identifier is impossible, moreover these acts allow the use of only one identifier on an identification document, etc.),

Other relevant legislation includes:

- Government decree 86/1996. (VI. 14.) on the protection of security documents
- Act LXXIX of 1993 on public education (regarding the ten digits pedagogue and student identification number.)
- Act LXXX of 1993 on higher education (regarding the higher education student identification number.)
- Act XXXV of 2001 on electronic signature
- Act LXXXI of 2003 on the electronic administration process of firms and the electronic recognition of firm documents amended by Act V of 2006 - effective from 1 July 2006)
- Act CXL. of 2004 on the general rules of public administrative procedures
- Act CXL. of 2004 on the general rules of public administrative procedures and services
- Government decree 17/2005. (II. 8.) on the students' card
- Government decree 193 of 22. September 2005 on the detailed rules of electronic administration
- Government decree 194 of 22. September 2005 on the electronic signature used in public administration procedures and the certificates thereof, and the requirements for certification service providers issuing the certificates.
- Act V of 2006 on administration of companies

3.3.3 Technical aspects

Most of the eGovernment applications can be used anonymously. However, some can be accessed only though the Client Gate. The data of KEKKH (the XR system) is provided directly on the Government Portal. The tax declaration system (eBev) has it own path on the Client Gate with reidentification.

As stated above the student card is one of the first country-wide eID card system in the world, but it has a ten years old technology (the PKI is only for the closed user group of teachers and administrators), so it is has no relevance in this topic.

The student card system has a common, country-wide middleware, however the authentication and administrative applications are local.

There is no any real eID card system in Hungary for the eGovernment. The Client Gate applies username and password, but in case a national eID card will be introduced, the Client Gate will use hard PKI based identification also.

The personal identification documents have an ID1 format but without chips. (The passport is an exception as far it is in the traditional ID3 booklet format, but there is a contact less chip in it with biometrical data. The technology is similar applied by other Member States.)

3.3.4 Organisational aspects

The Governmental Portal with Client Gate is managed by the Electronic Government Centre (EKK) of the of the Prime Minister`s Office and operated by a 100 percent state company, Kopint Datorg. The 270 Document Offices in the country are responsible for the registration.

3.4 Interoperability

As stated above there is no eGovernment eID at this time. Non Hungarian citizens can register for the Client Gate by appearing at a document office with passport, or apply for SIS or student card.

3.5 eIDM Applications

See description of the Client Gate above.

3.6 Future trends/expectations

Hungary was one of the first who introduced the card form tokens, as far as the student card was introduced in 1978. It is widely used for identification purposes for the age-group of 6-14 and its electronic form in the higher education. The nation-wide, spreading use of the school-network (Sulinet) could justify the use of eID for authentication of the higher education student card for lower ages too. The initiatives for the modernisation and for the widening of the group of users were unsuccessful on government level in the last three years.

Similarly there are various plans about the health cards or common citizens' cards, however Hungary should be cautious and wait both for the European standardization concerning the technical details and the common legal regulations.

The newest plans are about a multifunctional eID with digital certificates for electronic signature and authentication for eGovernment purposes but besides that there is potential usage for the card in eTransportation, eHealth, eCivial Servant and eStudent issues.

The 2 cards with the biggest potential to become the national eID card are the national ID card and the health insurance card.

As the EU structural funds opened up for the new member states there is a financial basis for the introduction of the new multifunctional card.

The basic obstacle in the way of introducing a multifunctional card by now is not financial but data protection and not enough cooperation in the administration.

3.7 Assessment

The basis of the national eID infrastructure with the Client Gate exists. Any international system planning to interoperate with Hungary will interoperate with the Client Gate which recently uses username-password based identification but as soon as a national eID card will be introduced will also use hard PKI based authentication.

One of the speciality of the Hungarian eID system is the earlier detailed reidentification method thatis used for identification in case of the Client Gate and in case of PKI based identification also. The possibility of the interoperability of this method on an EU level is questionable especially in case of PKI based identification.