doi:10.2498/cit.1001087

Improving the Security Levels of e-Government Processes within Public Administration through the Establishment of Improved Security Systems

Andrea Kö[1] and Bálint Molnár[2]

[1]Corvinus University of Budapest, Hungary
[2]Corvinus University of Budapest, Information System Department, Hungary

Processes that are related to the identification and the authentication of persons and other legal entities have been necessarily existing and functioning for a while in public administration and business. Information Society offers new e-services for citizens and businesses, which dramatically change the administration and results in additional challenges, risks and opportunities. Citizen's confidence and trust in services has to be improved, meanwhile several requirements, like personal data and privacy protection and legal requirements have to be satisfied. The usual business process of identification of the corresponding entity is generally based on some trivial control mechanism, typically password identification. In order to keep the trust of the public in the public administration activities, the process for entity identification (both person and legal entity) should be amended, taking in account the business and security consideration. Identity management solutions show intriguing variation of approaches in Europe, they are at a different maturity level of services.

Our paper gives an overview about the most frequently cited identity management architectures (namely: Liberty Alliance Architecture, Sibboleth, Government Gateway Model and Austrian Model) and presents an identity management framework (based on the PKI, but improved it), customized for the Hungarian specialities, which offer possibilities to improve the related services quality.

We give an overview about the decisive identity management approaches and we suggest an identity management framework (based on the PKI, but improved it), proposed as a general solution. The concrete example as a case study demonstrates a solution customized for the Hungarian specialities. Our paper shows a solution for the improvement of the identity management in e-government processes through the development of security mechanisms making use of the readily available technologies. The improved business and technology processes are demonstrated through the Hungarian solution to the problem as a case study.

Keywords: Public Key Infrastructure, e-government, security, digital signature, e-ID, smart card

1. Introduction

Tasks related to identification and authentication of persons and other entities have been a significant part of general business processes in public administration and business life. Information Society offers new e-services for citizens and businesses, which dramatically change the public administration, and at the same time, bring about additional challenges, risks and opportunities. Citizen's confidence and trust in services has to be enhanced, meanwhile several requirements, like data protection, privacy and legal requirements have to be satisfied. The traditional methods being in use now are neither secure nor comfortable. Amongst other, these are the reasons that explain identity management popularity. Several research projects are addressing identity management-related issues, like Guide [4], Prime [11]. PKI architecture can be one of the suitable candidates to enhance the level of security, meanwhile compliant with additional users needs.

The PKI architecture provides services that are rooted in the available IT technologies. The services implicate business process, directly or indirectly. The existing business processes should be aligned with the services of PKI that enforce some business and IT architecture and approaches for making use of technology. However, the basic issues, namely concepts related to identity management: the identification, certification, authentication of persons, and moreover the business processes involved in the previously mentioned activities own an interpretation in common sense that is not bound by the constraints and limits of technology. Regarding the whole bunch of business processes associated to PKI, we should investigate the requirements for process improvement, the opportunities for enhancing the currently existing business and software processes.

The challenge is that even if the more modern PKI technology is used, PKI itself cannot guarantee the authentication and authorization of the identity at the level that is anticipated by the public administration. Both business process side and the supporting IT technology for e-government services should be re-engineered; the available technology solutions should be complemented with appropriate parts.

The basic problem that should be solved somehow is the following: in the relationship between the citizen and the public administration, there is a very strong requirement for mutual verification and validation of the identities of partners, usually prescribed by the law, by the legal environment and by the jurisdiction. The most important Hungarian regulation approach can be found in Ket (CXL. Law, 2004). Ket covers the regulation about the way how to handle the linking of government to citizen (G2C) and vice versa, furthermore it codifies the rules for e-government processes and procedures. It is applied as a legal framework for business processes, procedures and standards within Hungarian public administration. Regarding the available technologies, there are several opportunities to implement a proper technical solution. However, a technically satisfying solution could collide with the legislation environment and jurisdiction. In some countries, the law permits a *de facto* central register of electronic identity of citizens; in other countries, either the laws in force or the practice of jurisdiction prohibits centralization of the registered electronic identities, and allows only some kind of distributed solution. The technology should provide services even in distributed or federated cases thereby the partners — the public administration and citizen — could build up a trust relationship mutually. The identity of citizen proved by a certification of PKI technology and issued by a commercial organization — the Certification Authority — could not be regarded convincing enough for the public administration. The certification contains some kind of name or names, but it does not have enough information for unambiguous authentication.

Our paper gives an overview about the decisive identity management approaches and we present an identity management framework (based on the PKI, but improved it), proposed as a general solution. The concrete example as a case study demonstrates a solution customized for the Hungarian specialities.

The outlined approach provides a solution among the constraints raised by the legal environment and the available technology, and avoiding some pitfalls that apparently yield a resolution but it hides some traps because disregarding the basic principles of cryptography. The solution is at higher security level than the traditional ones, and it even develops further the available PKI technology approaches providing improvement in the business process and supporting technology related processes and the applied software environment.

2. The Opportunities for the Improvement of Identity Management in an e-Government Environment

Within a corporate environment, identity management is dealing with managing the type of information, which is available for a certain application [7]. It involves maintaining a person's complete information set, spanning multiple transactions and contexts. Identity management application is part of an end-to-end security solution and addresses the needs for certainty in the areas of authentication, access control and user management [5]. Identity management systems allow people to define different identities, roles, associate personal data to it, and decide about access control of them and when to act anonymously. An identity management system would empower the user to maintain their privacy and control their digital identity [7]. The next business drivers of identity management are cited in the literature [5]:

- Cost reduction (unsatisfactory management of identity can increase the cost (e.g. waiting for permissions, etc.)).
- Increased security (inadequate access rights can be an additional risk for an organization).
- Increased compliance (an identity management system can help the organization to comply with laws (e.g. data protection laws) and regulatory environment).
- Increased usability (users are able to control their working environment and customize it).
- Infrastructure consolidation and application development speed (solutions can be built more rapidly, with applying reusable security elements).

Two major areas are distinguished in identity management; namely, enabling user access (authorization, authentication, etc.) and user life cycle management (user administration, provisioning, etc.). Another view is user's perspective (focus on efficiency (one single sign-on to many applications)) vs. administrator perspective (focus on efficiency of management) aspect. Major building blocks of identity management are the enterprise directory services, authentication, access control, and user management (ITGI, 2004). Four elements manage the whole life cycle of the identity within an organization, from creation to termination.

- The **enterprise directory** service consists of two major components:
  - *Directory services database* that operates as a hub data store for identity and authentication information.
  - *Meta-directory*: Its major functional service is to share identity-specific data, to carry out data synchronization among various directories, databases and applications within an organization.

Authentication is the procedure that checks the identity of a user so that he or she may have the right to use some resources and the access rights can be granted or denied correctly. The aim of **access control** is to guarantee that users are provided access only to those applications or resources they are permitted to use it some way. **User management** as IT function is responsible for providing user identities across multiple applications or systems.

Most important requirements against identity management are functional services and privacy [7]. Another important aspect which has to be emphasized is personal data and privacy protection. For the e-government services, the identity management solution elaborated in the past that are in use within corporate environment must have been, in principle, a perfect technological solution. However, several pre-conditions for a full–fledged application should be satisfied.

The foundation of basic technological architecture for the identity management is laid in Public Key Infrastructure. The basic principle is that the subject of identity management owns a key-pair: a public key and a private key. Even if the subject jealously guards his/her private key and publishes his/her public key, it is impossible to prove that the published key really belongs to the person who claimed it as his own. For this problem, a trusted business process was needed that "permanently" links the owner's identity to the public key. Thereby, a trust hierarchy came into life. The point of trust would bind public key to an identity (and maybe other personal information) on behalf of the owner of the key-pair. Everybody could then accept the single point of trust as a reliable authority that links the end-entity (person or legal entity) identity to the key-pair and the certificate that contains information about the owner and the public key.

The degree of validation at a reliable trust point, at Certification Authority (CA), can be reflected using extra information embedded into certificates: typically validation takes place at the level of e-mail address, in a corporate environment against the Human Resource directory, face-to-face meeting with additional checking of official credentials (passport, personal identification document, driving license, social security data, tax authority's identification number etc.)

However, even if the strongest authentication method is used for validation, the published information either in a certificate database or in the owner certificate represents only a small part of data that would be interesting, required by and significant for the partner who would like to identify the owner of the certificate and to verify. Generally, the certificate contains an e-mail address, a personal name, maybe some other names, and the public key. The certificate database that is publicly available may provide access only to the personal name, and downloading the certificate containing the public key, nothing less. Nevertheless, it may seem surprising that so little data are available for identification, but the anxiety for privacy and the attacks manifested during the past years justifies this practice. Based on agent and artificial intelligence technology, several soft bots ("software robot") were created to collect information from public Web sites as e.g. directory services for using the acquired e-mail addresses for generating spams, unsolicited e-mails. The only escape route is to avoid capturing of e-mail addresses by this easy way and against the owner original intention is using "*captcha*" like e-mail addresses. To protect the other personal data, the only solution is not to publish at all on publicly available Web sites, directory services.

The Certification Authority may have a paper or electronic database that contains the data that were checked during the validation process. The personal data and privacy protection acts in EU and the member states support this practice. However, the public administration in an e-government process needs much more information for an accurate identification of the owner of a certificate and a key-pair. Putting it simply, the question for the public administration is: among the several John Doe who is the right one?

The direct access to the database of personal information stored at the Certification Authorities raises security questions. If the public administration can retrieve data from this protected database, then anyone could do it. The previous issue leads to the common identity management processes:

1. There must be a functional capability for individuals to authenticate themselves with applications.
2. When identity data is passed from one country to another, it is likely that data conversions will have to be applied. This could be done by semantic integration and metadirectory services. As an example, last names of persons in Ireland stored in a directory should be mapped to last names of persons in Spain in the appropriate directory, and vice versa. To avoid interfering with principle of subsidiarity, these services are likely to operate on the basis of a common data model with mappings of this common data model to and from the data models of each single member state.
3. There should be some function of the directory service that retrieves the addresses or links of those services that want to interact with each other. A local authentication service may have to redirect an authentication request to the authentication service being cognizant.
4. Finally, legislation may require the existence of logging and notification services.

The problem can be formulated in the following way: the public administration requires a strong identification and authentication mechanism for its partners, in spite of the personal data and privacy protection obligation of government. How can we improve the business process for identity management for the purpose of e-government?

Approaches of IdM architectures show heterogeneous picture, we discuss briefly only the most frequently cited ones, namely: Liberty Alliance Architecture, Sibboleth, Government Gateway Model and Austrian Model, in order to compare them with the Hungarian approach.

2.1. Liberty Alliance Architecture

Liberty Alliance [13], a consortium representing organizations from around the world, was created in 2001 to address the technical, business, and policy challenges around identity and identity-based web services. The goal of Liberty Alliance is to enable consumers, citizens, businesses and government's online transactions applying open standards while protecting the privacy and security of identity information. All kinds of identities are linked by federation and protected by universal strong authentication, are being built with Liberty's open identity standards, business and deployment guidelines and best practices for managing privacy.

It offers the technology, knowledge and certifications to build identity into the foundation of mobile and web-based communications and transactions. Liberty Alliance Architecture is widely applied and cited in the area of identity management. The following part of the section provides a brief overview of the Liberty Alliance's federated network identity management architecture's components and the main features of the components. A high-level overview of Liberty Alliance Architecture modules can be seen in the following figure:

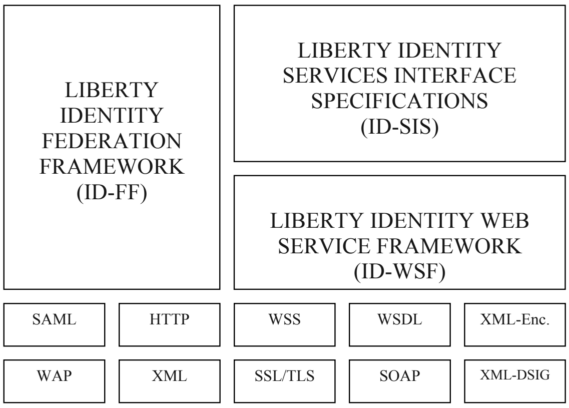

LIBERTY IDENTITY FEDERATION FRAMEWORK (ID-FF)
LIBERTY IDENTITY SERVICES INTERFACE SPECIFICATIONS (ID-SIS)
LIBERTY IDENTITY WEB SERVICE FRAMEWORK (ID-WSF)
SAML
HTTP
WSS
WSDL
XML-Enc.
WAP
XML
SSL/TLS
SOAP
XML-DSIG

Figure 1. High-level overview of the Liberty Alliance Architecture.

Main modules are the following:

- Liberty Identity Federation Framework (ID-FF)
- Identity Services Interface Specifications (ID-SIS)
- Liberty Identity Web Services Framework (ID-WSF).

Liberty Identity Federation Framework empowers identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management. The Liberty ID-FF module supports the federation of identities, including the corresponding management. This framework enables the interoperability of the most varied platforms and defines the federation for PCs and mobile devices (mobile phones, PDAs etc.). With ID-FF, the user has access to Single-Sign-On in his/her personal CoT ("Circle of Trust"). The ID-FF module also defines the exchange of metadata. The ID-FF module is the central module of the Liberty specifications.

Identity Services Interface Specifications is based on ID-WSF and contains specifications for the following functions: user registration, address book, calendar, location-specific services, and alarms ("alerts"). Liberty Identity Services Interface Specifications (ID-SIS) enables interoperable identity services such as contact book service, geo-location service, presence service, personal identity profile service, and so on.

Liberty Identity Web Services Framework (ID-WSF) provides the framework for building interoperable identity services, identity service description and discovery, permission-based attribute sharing, and the associated security profiles. ID-WSF, Identity Web Services Framework, is based on ID-FF and forms the basis to provide personified services. ID-WSF includes:

- the exchange of individual attributes ("permission-based attribute sharing"),
- the collection of identity elements in a distributed environment ("identity service discovery")
- interaction services ("interaction services") additional security profiles, which are to be observed during data exchange ("security profiles")
- "Simple Object Access Protocol Binding" (SOAP binding)
- "extended client support" (extended support for end devices, not IP/HTTP specific)
- "Identity services templates" (personality profiles specification).

Underlying part of the architecture – extension of industrial standards represents a collection of international standards relevant to Liberty. ID-FF, ID-WSF and ID-SIS are based on these standards. These refer to existing standards; as necessary and when required, they will be extended and approved with the appropriate standardisation organisations. Liberty Alliance works together with many organisations; some of them are:

- Organisation for the Advancement of Structured Information Standards (OASIS)
- World Wide Web Consortium (W3C)
- Internet Engineering Task Force (IETF).

The following are used as standards: SAML, HTTP, WS-Security, WSDL, XML-ENC, WAP, XML, SSL/TLS, SOAP, and XML-DSIG.

2.2. Government Gateway Model

The goals of the model were to make all Government services accessible on-line by 2005, provide universal access to the Internet and ensure the UK is the best place in the world for e-commerce [4]. Government Gateway is the common channel linking the public with government systems via Web sites, government portals and Internet-enabled applications. It is designed not only to benefit government and public sector departments, but also three million UK businesses and 60 million citizens. Main features of the gateway model are the following:

- Aims to centralise authentication of citizens and businesses
- Heavy PKI origins - costly and complex for users, low take-up
- Looking to ease user registration and increase take-up
- Have registration & enrolment process.

Government Gateway provides a secure, easy-to-use means for people and businesses to enrol for services and file forms including income tax and value-added tax returns. Anyone able to use a Web browser can access the system, and it is easy for the Government to operate, manage and maintain. When launched, the UK online e-government initiative faced challenges in addition to connecting a huge number of users. It had to integrate a single access path, serving all users, with departmental IT infrastructures that had operated independently for many years. The role of the Government Gateway is to provide departmental systems with an outward-looking perspective, responsive to the needs of individual citizens and businesses of every size and type.

2.3. Austrian Model

By the Austrian e-government strategy, the unambiguous and secure identification of citizens/ businesses and administration units as communication partners is a decisive factor implementing e-government services. Therefore electronic signatures – in some sensitive cases secure or "qualified" (by the EU directive notion) electronic signatures – are required for communication to public administration.

The Austrian government has got a software application developed for a middleware – it is called Security-Capsule – which is the link between different signature tokens (smart cards, USB-Tokens, mobile phones) and the various e-government applications.

The sectors of public administration that offer smart cards (e.g. Social Security Authority, Passport Office, Banks, teaching institutions), can integrate this software into their e-government related services and converting the smart cards or tokens issued by particular sectors of public administration to official citizen cards, which can be used in all e-government processes.

In the Austrian approach, the use of smart card and PKI technology is intertwined in an inseparable way. The smart card or token can be any type of their genre, assuming that it is suitable for storing a digital signature certification. This principle makes allowance for using the smart cards/tokens issued by various sectors of the Austrian government as e.g. the Social Security, National Health Service and by other governments of EU member states to use uniform way. For the use of the smart card/token in relationship with the Austrian public administration, a specific registration procedure is required. During a registration procedure on the smart card token, two key pairs are stored (A-key-pair for "secure or qualified" signature and B-Key-pair for an advanced digital signature), and, furthermore, a person identifying data tuple. The data tuple consists of a unique identifier of the person ("Basic Concept"), the public key of the digital signature on the smart card, public key of B-Key-pair, the "valid through" data and the whole tuple is signed by the proper authority. The tuple on the smart card will be used as a person binding, i.e. a one-to-one and unambiguous mapping between the person and the smart card that ensures that only the owner of the smart card and having the knowledge of the password to the smart card can act on the behalf of the particular person. In principle, the sector specific identifier within the public administration differs in each sector of public administration as the procedure for generating it makes use of the basic concept, the character string as the denomination of the certain sector of public administration.

During the procedure, these data is fed as input to a hash function — that does not have an inverse function — constructing the required identifier. In this way, the person is identified in any official procedure by the person binding and his/her digital signature on the document. The authority can unambiguously identify and authenticate the person through this information. There is a well-elaborated mechanism for a trusted hierarchy assigning the legal responsibility to another person or legal entity to act on behalf of the person in official procedures of e-government services.

The communication between the person as a client in the sense of IT and the e-government services takes place in a secure format using proper protocols as SSL, TSL. In each official procedure, there is a front-end for security control, the so called Security Entrance, that provides the necessary checking for the following information item as the digital signature, client credentials, identity checking through the person binding transmitted, deducting the procedure-specific-identifier for the particular official procedure; and, if necessary, the assignment hierarchy for legal responsibility.

At the interface of an e-government service provider, the identification mechanism uses a cryptographically safe SSL communication tunnel. Initialising the SSL connection, the public key of the smart card is used to build a data block for authentication. Thereby, at the same time, the client, the browser and the person are authenticated, and made unnecessary to exploit the User-ID and password, assuming that the integrity of the card in the sense of cryptography is ensured.

At the basis of the Austrian e-government workflow are XML-forms provided by online applications via a central portal, which can easily be displayed by the web browser. If preferred by the user, some fields on the form can be filled in automatically because of the Security-capsule which stores personal information of the cardholder (e.g. name, birth date, ID-number). The data for the remaining fields needs to be provided by the citizen. If necessary, attachments like birth certificate or electronic payment confirmations can be added. Upon completion of the form, the Security-capsule requests the citizen to sign with the citizen card. After the entry of a PIN number, the complete form is delivered to the back office application. When the back-office process is concluded, the administrational notification will be electronically signed by the authority, encrypted with the citizen's public key and delivered to the citizen's electronic delivery service. Comparison of the above described IdM approaches is demonstrated in the Table 1.

2.4. Shibboleth

Shibboleth is an Internet2/MACE project developing architectures, policy structures, practical technologies and an open source implementation to support inter-institutional sharing of web resources with access control requirements. It uses SAML as an underlying technology. The Shibboleth project also created OpenSAML, an open source implementation of the SAML specification. Shibboleth is a federated approach to attribute sharing. It enables resource sites to request attributes about a visiting user from the users' origin site. The origin site must know its users and be able to authenticate them. These attributes can then be securely transferred to the resource site. It is up to the user to specify which information can be released about the user and to which site. It is possible that resource sites only receive a small set of attributes about a given user (e.g. the location) and do not get to know which particular user it is, and thus Shibboleth is seen as a privacy enabling technology. Shibboleth is aiming to solve the needs that universities typically have, but it is not restricted to that domain in its use and application. It has the potential to be used much more widely as a single-on or privacy enhancing technology.

3. Service Requirements against PKI Infrastructure Enforced by Business Processes of e-Goverment

There are several requirements against the identity management and electronic signatures that cannot be satisfied with the recently available technology, however the common sense and the normal business logic seems to anticipate as a requisite of the service set to be provided.

	Liberty Alliance Architecture	Shibboleth	Government Gateway Model	Austrian Model	Hungarian Model
PKI enabled	yes	yes	yes	yes	yes
Standards applied	SAML, HTTP, WS-Security, WSDL, XML-ENC, WAP, XML, SSL/TLS, SOAP, XML-DSIG	HTTP, XML, XML Schema, XML Signature, SOAP, SAML	HTTPS, SOAP, XML Schema, COM/XML	TSL, XML, SAML, HTTPS	LDAP, SSL
Sector Orientation	Business, Public	Public	Public, Business	Public, Business	Public
Opportunity for Verification of the Supplied Data	Partly Supported	N/A	Supported	Supported	Supported
SSO (Single Sign-On)	yes	yes	yes	yes	yes
Digital Traceability	No	N/A	Weak	No (In principal, but there is opportunity for surprise attack)	No

Table 1. Comparison of the IdM Approaches.

Identification of the owner — (the *end entity, EE*) — of a digital certificate does not cause problem in a closed business world or in a relatively narrow trust community, where the personal details and the content of the digital certificate can be mapped to each other with little effort. Nevertheless, the e-commerce and the public administration of a nation (e.g. tax system) oblige the unambiguous mapping the identity of the cyber entity embodied by the digital certificate and the end entity as it exists in the business life, the real world and in the relationships with the public administration.

Basic elements of PKI architecture are the **Registration Authorit**y and the **Certification Authority**. These two components are exactly mapped to two disparate software constituents of the IT architecture that are typically licensed separately. The explanation is that the underlying organizational architecture and the IT solution are strongly coupled to each other.

Thereby, in a PKI environment, there is an *RA* (*Registration Authorit*y). The end entity submits its details through RA to the *Certification Authorit*y (*CA*). The RA performs some checks on the validity of the supplied data, and then the RA gets a unique identifier code and the public key written in the certificate instead of the user-specific information. The data stored within the end entity's certificate are supplied by CA through a secure channel to the *RA*. The end entity possesses its private keys that are tied to the public key contained in the certificate; the ownership of the key-pair by the end entity cannot be questioned rightfully. The PKI system, the *CA* and *RA* together ensure that the user-specific details are publicly not available and accessible, and not even published in the certificate. However, the *CA* is able to provide verification information about the identity of the end entity, and some details of data of *EE* for an enquirer supplying e.g. the unique identifier code from within the certificate.

The queries raised by an enquirer could seem as if "someone presented an end entity certificate containing the following unique identifier and/or public key, and claiming, in an attached piece of information, to be John Doe; or claiming their postal address is No. 1 Any Street, in Anytown — is this true?" The enquirer can be a business partner, an agent or client representing public administration, and has the right to request directly from the end entity further piece of information, moreover makes use of their own databases containing legally stored, not public information about the end entity. The agent can match the information coming from different sources namely, the CA/RA, its own databases and the end entity. The available data can be matched, verified and validated algorithmically proving or disproving the identity of the end entity. This solution can be named as "Identity background checking",

A closely related issue is the management of the Certificate Revocation List (CRL). The validation service in a PKI environment is very similar to the very early credit card companies' solutions whereby a list of cancelled cards — for whatever reason — was regularly distributed to the business partners. The burden of checking and controlling that an issued digital certificate is used rightfully, conforming to the intended policy, regulation and specific authorization is on the recipient (the relying party). The recipient should check whether the user's trusted status has been revoked by the issuing CA or not. The issuing CA regularly creates a CRL that identifies its revoked certificates (regardless of their possessing valid expiry dates, attributes and signatures). A CRL is dated, and then signed, by the issuing CA to show its authenticity and is issued perhaps on an hourly, or daily basis. The CRL has a fixed validity period as well.

The recipient, the relying party uses the logical decision "IF a certificate is not included in the CRL THEN it is OK". This logical inference uses 'the negation as failure' or 'the closed world assumption' that is well-known in the logics of mathematics and computer science/informatics, and legally applicable when no other reliable information source is available. For security reason, the only correct logical conclusion that can be drawn is "IF certificate is listed in the CRL THEN it is NOT OK".

There is some technological solution, but because of the lack of the accepted business model and the mutually beneficiary financial solution, some extra technological burden should be undertaken, the solutions are not very widespread. The on-line certificate status protocol (OCSP) allows certificates status to be validated in real time. The content of the answer is generally constrained legally to "YES" or "NO". CRL to be advertised, there is no need for the application of "the negation as failure" logic. The content of the answer is generally constrained legally to "YES" or "NO".

The simple Certificate Validation Protocol (SCVP) is a similar approach to OCSP, but it permits for the relying party to get rid of much of the certificate chain checking work and pass it to the SCVP responder. Responses could be more than "YES" or "NO" if it is legally acceptable to provide more detailed information about the user/certificate owner who has elicited the query on the side of the enquirer.

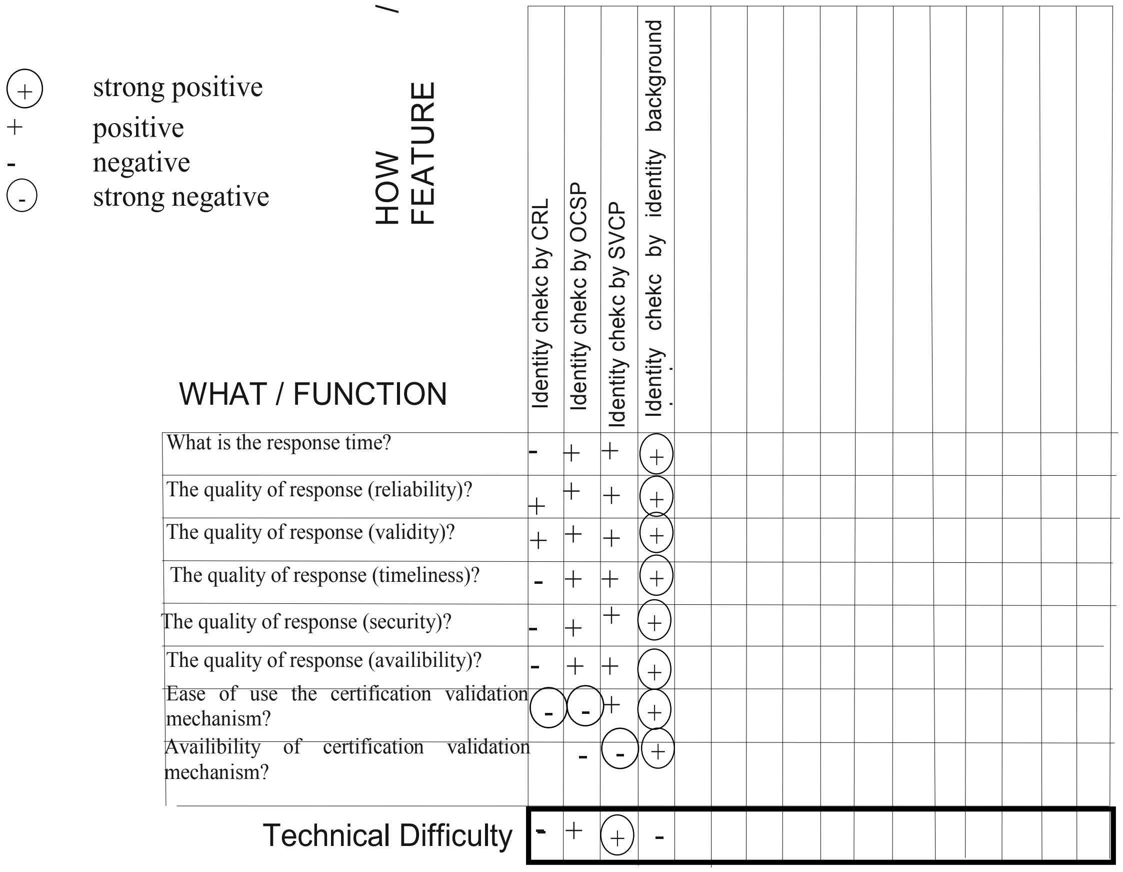
Based on the requirement analysis described above and illustrated using the QFD approach (Quality Function Deployment) in Figure 2, the conclusion can be drawn that the viable and feasible solution regarding the state-of-the-art of PKI is the identity background check that could be implemented in a reasonable time-frame and could fit into the public administration and currently available PKI framework.

4. The PKI Technology as a Viable Tool for e-Government — Arguments for the Solution Selected for the e-Government in Hungary

For political and economic reasons, there is a strong pressure to implement more and more public administration services using information technology appearing as e-government services.

The remote access to the e-government services makes it necessary that the citizen should identify and authenticate itself by a reliable and secure manner that ensures mutual trust for both public administration and the citizen. However, we have to talk about client or end entity instead of citizen as not only natural persons but other legal entities may have contact with the public administration.

In the commercial world and within single organizations, the PKI technology developed during the last decades has achieved success. However, the PKI technology has accomplished only modest success in the relationship between client and public administration in the form of e-government. In the various form of contact between the clients and government, there is a very critical and significant difference to the



⊕ strong positive
+ positive
- negative
⊖ strong negative

WHAT / FUNCTION	Identity chekc by CRL	Identity chekc by OCSP	Identity chekc by SVCP	Identity chekc by identity background
What is the response time?	-	+	+	⊕
The quality of response (reliability)?	+	+	+	⊕
The quality of response (validity)?	+	+	+	⊕
The quality of response (timeliness)?	-	+	+	⊕
The quality of response (security)?	-	+	+	⊕
The quality of response (availibility)?	-	+	+	⊕
Ease of use the certification validation mechanism?	⊖	⊖	+	⊕
Availibility of certification validation mechanism?		-	⊖	⊕
Technical Difficulty	-	+	⊕	-

Figure 2. QFD for requirement analysis of the technical solution for identification approaches.

use of PKI by enterprises, especially the internal utilization of PKI for the secure and reliable communication and business management among the staff of the organization.

The definite difference is the privacy and protection of personal data. A person can be identified unambiguously or with high probability by using some natural bits of information as e.g. the given name, second name, date and place of birth, mother's maiden name, and home address. There are some identification numbers or character strings used within certain sectors of public administrations as tax number, social insurance number, personal identification number, etc. Although these unambiguous and easy-to-handle identifiers cannot be used together because of the legal environment in some countries and jurisdiction, they cannot be stored in the same data store and cannot be linked to each other. With slight differences, this statement is valid largely for the member countries of EU.

Within a certain organization for internal use, the content of digital certificates and data related to the person owning the certificate does not create conflict regarding the privacy issue. The digital certificates and the other data are published in a public data store; in a directory that is typically realized by the LDAP (Lightweight Directory Access Protocol), technology could be accessed and read by other members of the organization. The typical data that occur in this context are the e-mail address, the personal names, titles, job description, department name, telephone numbers, etc. The access to this type of data for other members of the organization is very important for business reasons, to support the workflow and business processes. For general public, to publish only restricted set of the before-mentioned data set has been crushed by the spam. The appearance of other personal data on public LDAP servers would hurt more or less the privacy of persons, naturally depending on the local jurisdiction. To make this point clear, some legal rules for the public administration in Hungary consider the name and official telephone of civil servants as a public data. Whether the e-mail address is personal or public data depends on the uniqueness and dependence on the individuality of person, maybe the e-mail provided for official use is public data, but other e-mail addresses should be considered as personal data. The debate on this topic is continually carried on, and still has not been concluded.

If a citizen as a client of the public administration acquires a digital certificate from one of the commercial certification authorities (CA) for managing his/her own business with the public administration then the public directory of the certification authority will not contain other data as the name of the citizen and digital certificate containing the public key. Moreover, the directory (e.g. LDAP technology directory) may hold an e-mail address that is strictly coupled to the digital certificate. Optionally, the directory record may include the name of organization, department/business unit, country code, identification number/serial number, name of city or town may appear as public information. But the publication of these data is a little bit risky because of privacy issues, unless the person has given permission for the publication. The public key and the serial number of the certification at a particular CA can be considered as an unambiguous, unique identifier of a person. For identification and authentication, these data seem to be perfect, from both view points of the public administration and information technology. Though, what does the public key identify? The popular view is that the person is identified. The question is which person is identified. Using public key included in the certificate, only the name and maybe the e-mail address of the person are public. What is the process that can identify unambiguously the person on the side of the public administration in this situation? Because, generally, the available information is not sufficient for the unambiguous identification as the names (given name, second name, etc.) are not unique. The e-mail address is unique but there is no mechanism to map the e-mail address onto a person. The alternatives for public administration are the following:

1. The public administration creates a central database of e-mail addresses and couples them to certain persons.
2. The public administration creates a central database of public keys and links to certain persons.
3. The public administration uses the existing central databases of tax numbers, social insurance numbers and personal identification numbers. A person is unambiguously mapped onto the identifier in each single database. The identifier and public key should be linked together in each database.

Disregarding the Big Brother approach that the state collects all personal data, one of the lawful solutions is a voluntary registration mechanism when the person and his/her public key within the digital certificate are linked together. The major task is to find a registration, certification, identification and authentication mechanism which conforms to the international (EU) directives and national laws and regulations. Several countries in the EU have a central registry of citizens in the form of databases and their permanent and maybe temporal address. The tax offices, the social insurance agencies have similar databases containing the identifier that is specific to the sector, moreover several items of the personal data suitable for identifying the person and considered as a natural identifier. There is a temptation to use these databases to support the identification and authentication within each sector of public administration involved in the e-government using PKI technology. It seems a feasible approach to join the public key of a person's certificate and identifier specific to a particular sector of public administration. Arguing that "the public key" is public — nomen est omen — and there is no hurting the privacy of a person by this way. However, there is a serious logical fault in this argument. Through the public key of a person's certificate all the separate and insulated databases could be joined together by a primitive algorithm without any serious effort. All the activities related to the public administration of a single person could be tracked easily, and the data collection about a person would become trivial. In EU generally and in the member states especially, this solution is strictly prohibited by the law and the practice of jurisdiction. A following problem area is to support the commercial certification authority by creating market for their services. At the same time, the state, the EU member state should remain neutral considering the competition on the market ensuring market opportunity for the commercial organization. All the efforts to introduce the PKI technology to ease the tasks associated to the e-government concentrates on the resolution of above outlined conflict. The various

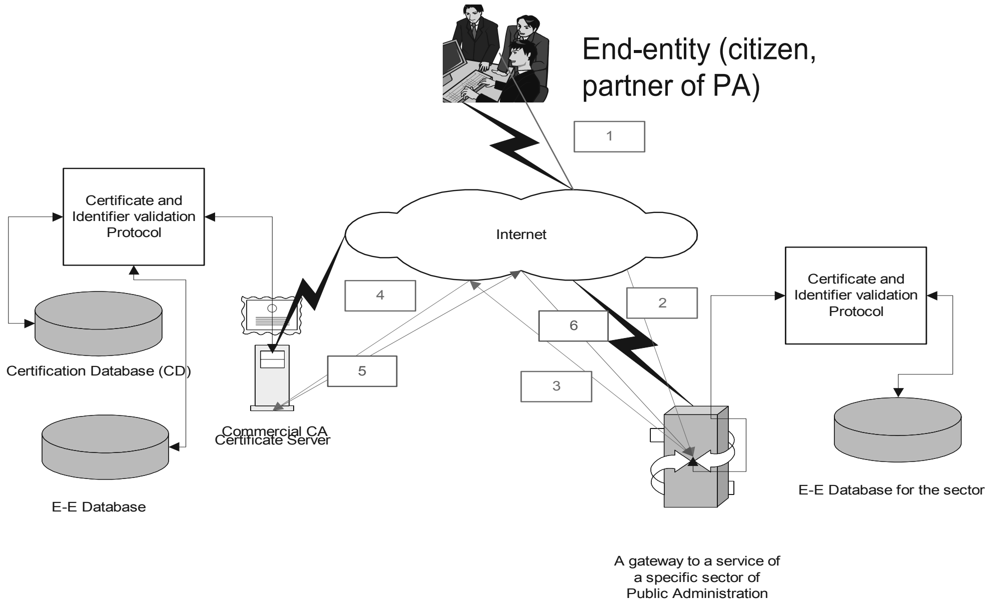

End-entity (citizen, partner of PA)
1
Certificate and Identifier validation Protocol
Internet
4
2
6
5
3
Certificate and Identifier validation Protocol
Certification Database (CD)
Commercial CA Certificate Server
E-E Database
E-E Database for the sector
A gateway to a service of a specific sector of Public Administration

Figure 3. Communication lines among the participating partners of mutually trusted e-government service points (numbers denote the order of the communication).

national models try to find an appropriate solution that satisfies both the technology and the legal environment.

5. The Hungarian Solution that Improves both the Service and the Security Level of e-Government Processes and Ensuring Privacy

In Hungary, the Gordian knot of the above mentioned problem is sliced to in the following ways:

1. The request for a certificate enclosing a digital signature and the registration with conforming rigorous Certification Policy (CP) at a commercial Certification Authority that enables the certification holder to do business with government through e-government services. Avoidance of centralisation of personal data is automatically guaranteed and designates a movement towards a federated PKI architecture.
2. At a single CA, the person's naturally identifying data is stored a secure database beside the certificate and the public data that will be published in a directory. The certificate contains an indicator that signals the appropriateness for public administration, to handle issues through e-government services. The identifiers specific to certain sectors of public administration (tax number, social insurance number, etc.) are not stored either in the certificate or in the personal registration database, not even some coded format that might be created by a cryptographic algorithm or a hash function.
3. The CA-s should own by the Force of Law a so-called CRL site. At this site, the CA should provide specific services that for an identification request from public administration answers by a "Yes" or "No". The CA receives a data package including the naturally identifying data of a person, public key and/or the serial number of the certificate. The service carries out a check on the database, retrieves information and unifies to the provided data. If there is a match the answer is "Yes", in all other cases the answer is "No".
4. During an interaction with public administration, a citizen can identify and try to get himself authenticated by a certificate enclosing a digital signature. The e-government service of a specific sector during the interaction requests the sector particular identifier (tax number, social insurance number), the public key of the digital signature, and some naturally identifying data. The e-government service — based on the gathered data — calls for an answer from the

certificate issuer CA and performs an internal check on its own internal database. After gaining an answer which is satisfying and fitting to the available data from both resources, i.e. internal and external, the person is authenticated, moreover authorised to execute transactions through the e-government service.

The above description conforms to the legal environment in Hungary embodied in the Act about the Processes of Public Administration (by the Hungarian legal acronym, Ket (CXL. Law, 2004)). The registration Authority is recently with **The Credentials Offices** run by local government. The *Credentials Offices* issue driving licences, personal identity cards and the electronic identifiers for "**Client Gateway**" of e-government in Hungary. The *Credentials Offices* create digital certificates for digital signature and electronic identity for those who request one. The basic principle in Hungary is the "**opt in**", i.e. the electronic identity — for a while — is not compulsory but optional. Now, it seems that two logical types for electronic identities and separate smart cards will be in operation in the near future in Hungary. There will be one for general personal identification and one for Health Insurance.

The *Credentials Offices* are linked to the **Central Registration Office for People and Addresses** on-line for sending the identification data and the checking happens in batch processing at the *Central Registration Office*.

6. Conclusion

The original aim of PKI technology was to provide services regarding identification, authentication and authorisation for e-commerce and for enterprises' internal IT infrastructure. Within the e-commerce, the PKI technology would have enabled that any contract would be unrepudiated and before the court it could have been enforced, it would have been especially important in the copyright-related products and commercial artefacts. Nevertheless, the various pre-payment method, bank card solutions, and direct transfer between the bank accounts electronically, furthermore the enhanced security of before-mentioned type of transactions played down the urgent need for application of digital signature and the related technology in practice. Together with the developed logistics of Post services, the e-commerce was able to increase its volume without the extensive proliferation of digital signature and PKI infrastructure.

For internal use of PKI within enterprises has got an impetus. The market leaders of software manufacturers on the office, document handling and e-mail technology have built in their product the major element of PKI technology as e.g. local Certification Authority, issuing certificates of digital signatures and identification, e-mail systems integrated with LDAP technology for storing the person's data. There are no legal problems with this approach as the publication of personal data happens within a restricted and closed community. The PKI technology in such an environment serves well the interests of enterprise workflow management, operates smoothly together with other software applications and, at the same time, ensures a secure, reliable and trusted IT environment.

On the other hand, the public administration faces lots of legal issues as the circle that may want to do business with it is not closed, it could be rather regarded open. The procedures of public administration obey to strict regulations, laws and other legal rules, for this reason the e-government service should find the narrow path between the legal opportunities and solutions provided by the PKI technology. The public administration is between Scylla and Charybdis.

The Austrian approach for utilizing the PKI infrastructure and the smart card technology for the e-government services is fairly sound. However, there are two minor faults.

The first one is that the whole procedure starts from a centrally stored identifying number, naturally there is a strong attempt using cryptographic methods to eliminate any trail that would help to reconstruct the original data. Though, the starting point is a central state register anyway, and this idea is not satisfying in several countries and jurisdiction regarding the personal data and privacy protection, privacy laws and regulations. The objections that are raised are worth considering in the light of 9/11 and afterwards the attempts for restricting the civil rights and extending the power of national security forces on the activities of data collection about persons even by liberal governments and jurisdiction.

The second one is more technical, namely the use of hash function for information protection. The original purpose of the hash function was to ensure the integrity of the data message, not for protecting the data from algorithmic attack. As the famous attack for password recovering in the UNIX systems demonstrates —the so called dictionary attack — if the structure and space message is known and constrained, the attack could be successful. The success depends only on the computing power uses up. The procedure to create the person binding and the sector specific identifier uses a hash function in the case of Austrian e-government. The data used as starting point and their structure are well known and publicized. Theoretically, there is a chance for surprise attack as there is no rigorous mathematical proof for the security of the hash function applied, and the hash function is used for other purposes as it was designed enhancing the potential threat and vulnerability of the method.

The Hungarian approach avoids several pitfalls.

1. There is no central registration of citizens acquiring certificates for either qualified or advanced digital signature.

2. The registration process does not use any sector specific identifier of the Hungarian public administration at the commercial Certification Authority. The central register of citizens and addresses could be queried by the person's naturally identifying data, and the central register responds only by a "yes" or "no", thereby supplying an enforcement of the authenticity of the transmitted data. The personal data, identifier stored in the central register do not play any role generating the certificate, the digital signature and the personalization of a token (smart card, USB token, etc.)

3. The certification issued by the commercial Certification Authority contains sufficient information for interfaces and automated software solutions at the various sectors of the Hungarian Public Administration to carry out the procedure for authentication and validation of the certificate of digital signature and other supplied and retrieved data from the databases of the particular sector of government. For example, the URL of Certification Authority where the data exchange could be performed.

4. The applied cryptographic procedures related to the PKI technology are the widespread, technically sophisticated, sound and according to the state of the art are reliable and resistant to the known algorithmic attack.

The Hungarian solution is technically sound and conforms to the legal environments without any compromise, for this reason it is worth considering to push the international proliferation of this approach.

References

[1] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2001, ISBN: 0849385237.

[2] Burnett, S., Paine, S., *RSA Security's Official Guide to Cryptography*. New York, Osborne/McGraw-Hill, 2001, ISBN 0-07-213139-X.

[3] Delfs, H., Knebl, H., *Introduction to Cryptography, Principles and Applications*. Berlin, Springer-Verlag, 2002, ISBN 3-54042278-1.

[4] Gateway to e-Government-Success Story, `www. gateway.gov.uk`, 2001, (December 18, 2005).

[5] GUIDE – Creating an European Identity Management Architecture for e-Government (FP6 IST project – Networked Businesses and Governments (IST-2002-2.3.1.9)), 2006.

[6] Herreweghen E. et. al., Enterprise PIM Roadmap „Privacy Enhancing Technologies and Identity Management Systems in Enterprises", manuscript, 2002.

[7] IDA Enterprise DG: Architecture Guidelines for Trans-European Telematics Networks for Administrations Brussels, September 2004.

[8] ITGI (IT Governance Institute) – ISACA (Information Systems Audit and Control Association): „Enterprise Wide Identity Management – Managing Secure and Controllable Access in the Extended Enterprise Environment", manuscript, `www.itgi.org`, 2004.

[9] Koch M., Wörndl W., Community Support and Identity Management. *Proceedings of the European Conference on Computer-Supported Cooperative Work* (ECSCW 2001), Bonn, Germany, September, 2001.

[10] NASH, A., DUANE, W, JOSEPH, C., BRINK, D., *PKI: Implementing and Managing E-security*. New York, Osborne/McGraw-Hill, 2001, ISBN 0-07-213123-3.

[11] PRIME - The PRIME project receives research funding from the European Union's Sixth Framework Programme and the Swiss Federal Office for Education and Science, (FP6 IST project – (IST-507591), 2006.

[12] STEVEN, J. R., *Identity Architecture*, Information Systems Control Journal, Volume 4, 2003.

[13] TEMPLE, R., REGNAULT, J. (EDS.), *Internet and Wireless Security*. The Institution of Electrical Engineers, London, UK, 2002.

[14] The Liberty Alliance,
`http://www.projectliberty.org`
(December 18, 2005).

[15] Shibboleth,
`http://shibboleth.internet2.edu`
(December 18, 2005).

Received: July, 2007
Revised: October, 2008
Accepted: November, 2008

Contact addresses:
Andrea Kö, PhD
1093 Budapest Fövám tér 13-15. II/225
Corvinus University of Budapest
Hungary
e-mail: `ko@informatika.uni-corvinus.hu`

Dr. Bálint Molnár
1093 Budapest Fövám tér 13-15. II/225
Corvinus University of Budapest
Information System Department
Hungary
e-mail: `molnar@informatika.uni-corvinus.hu`

ANDREA KÖ, PhD, is Associate Professor at Corvinus University of Budapest, Hungary. She has MSc in Mathematics and Physics from Etvs Lrnd University of Budapest, Hungary (1988), a University Doctoral degree in Computer Science (1992) from Corvinus University of Budapest, Hungary and a PhD degree in Management and Business Administration (2005) from Corvinus University of Budapest, Hungary. She participated in several international and national research projects in the areas of: identity management and IT audit; semantic technologies; knowledge management and e-government. She has published more than 50 papers in international scientific journals and conferences. Her research interests include business intelligence, intelligent systems, knowledge management, semantic technologies and IT audit.

DR. BÁLINT MOLNÁR graduated as mathematician at Eötvös Loránd University in Budapest. He received a PhD in technical informatics from the University of Technology in Budapest. He has been a lecturer at the University for more than 20 years, and he has worked as Associate Professor for more than 10 years. His research areas are: applied artificial intelligence, analysis and design methodologies for expert systems and knowledge intensive systems, e-government, information systems auditing. His educational activities cover the following areas: artificial intelligence, expert systems, e-government, information systems auditing and controlling, model-driven information system analysis and design (UML/UP and SSADM); furthermore, information system strategy planning, analysis, design, project management. At the same time, he works as principal consultant for Information Technology Foundation of the Hungarian Academy of Sciences. The Information Technology Foundation operates as service provider in ICT consultancy for the Hungarian Government. He took part in the preparation of the public procurement procedure for purchasing a PKI infrastructure for the Hungarian Government and in the project for implementation of both technical and organizational side.