Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Anonymous, Liberal, and User-Centric Electronic Identity – A New, Systematic Design of eID Infrastructure

Libor NEUMANN
ANECT a.s., Antala Staška 2027/79, Prague 4, 140 00, Czech Republic
Tel: +420 271 100 100, Fax: + 420 271 100 101, Email: Libor.Neumann@anect.com

Abstract: A systematic design of a new eID infrastructure has been carried out and partially verified. The decision to start the design from scratch was based on a critical analysis of the current and known eID infrastructures and tools, their limits, and comparison with current needs and the real world environment. The design is based on ideas of anonymous eID, liberality, and user-centric solution. New ideas improving security and privacy protection together with private data management are used. Also included into the eID design are modern infrastructure features like security management, ICT lifecycle support, and openness to future improvements.

The design and verification processes are briefly described together with the results achieved.

1. Introduction

An analysis of current eID architectures [1] shows that none of these fulfils all current needs of eID infrastructure stakeholders (i.e. customers and service providers). The systems were not designed to be used in worldwide public networks with billions of users and millions of service providers. None of the existing eID solutions is a truly up-to-date eID infrastructure supporting seamless and secure personified communication with all the needed features. A new eID design is needed that reflects current reality.

This paper describes an attempt to carry out and verify a new and systematic design of eID infrastructure. As the paper limits do not allow to describe and discuss all interesting and important questions in detail, only a briefly description is given

2. Objectives

The current eID solutions seem to have been built from the bottom up. They are designed to use specific technologies for eID solutions rather than to be based in a systematic top-down design of the eID infrastructure. Solutions for many important systematic issues are frequently missing or insufficiently supported. For instance, they tend to:

- Overestimate or ignore the skills of a regular user,
- Confuse physical identity with the need to distinguish between different remote users of electronic services,
- Use one technology or a single technology principle,
- Underestimate the need for eID infrastructure management,
- Not support the innovation cycle and future technology, and
- Give insufficient attention to protecting private data.

Based on a systematic analysis of existing solutions [1] (where the basic design targets reflecting current needs were formulated), an attempt is ongoing to come up with a new design for an up-to-date eID infrastructure. The design starts from scratch, and it is built from the top down in order to address all the various aspects of the solution. The design recognises and reflects the key stakeholders and their needs. The result is the proposed ALUCID® (Anonymous Liberal and User-Centric electronic IDentity).

3. Design Methodology

The design was carried out in a stepwise manner, starting from scratch, and it included relevant analysis and evaluation at each step.

The first steps were theoretically based. A very critical analysis was made that included scrutinizing the known eID architectures' weaknesses and strengths [1]. The historical environments that had existed during these architectures' designs were quite interesting, too, and these were able to explain many of the weaknesses. An analysis was made also of today's real world needs [1]. Six described common needs were used as design targets and basic evaluation criteria.

Also analysed were the limits that today's real world establishes. That analysis examined two different security domains in the current real world: the global cyberspace, with its billions of interconnected computers having continuously growing power, and the local human environment, characterised by very limited human skills and no possibility for its significant improvement. The existence of two domains with opposing security needs and resources was very important in the theoretical design.

The theoretical analyses yielded the first design principle, which is to using a specific personal device (i.e. a specific computer) to interconnect the security domains and separate the high-power, dynamically changing cyberspace from the conservative human environment. Current technology offers easily portable devices with sufficient computing performance that can be produced in the real word. The specific device has been named the "Personal Electronic Identity Gadget" (PEIG®).

The next design steps were focused more on details. A virtual machine design abstraction was used. The specific instruction set was designed to support basic functionality. The function was verified against the idea of very simplified use by the end-user. The organization of the eID environment was simplified as much as possible. All intermediates and all additional activities were deleted and automated by the virtual machines. Such new principles have been used as anonymous identity, symmetrical authentication, limited validity space of identifiers, and one-time identity. The design includes the dynamics of identifiers and secrets as standard features. Every identity has limited validity time and count and can be automatically changed without loss of the identity link.

Private data management – namely e-government supporting features – was part of the more detailed design. The questions had to be resolved of where the private data can be stored, how this data can be shared, and how to protect end-user privacy. New ideas were combined with such well-known principles as storing personal data only in secured information systems managed by skilled service providers, separating authentication from authorisation [2], "introducing PEIG" to the service provider or "remote heritage of PEIG introduction" supported by one-time identity.

The theoretical design was completed by the first description, whereby the main principles were described and include security management, a basic description of the virtual machine instruction set, and communication between virtual machines for all designed functionalities.

Verification by models and prototypes was the last design step. A global solution with limited technical details was verified by Model 1. The verification resulted in an improved virtual machine instruction set and clarification of interfaces, including interfaces between the standard computer and network environments. Model 2, then, was focused upon security algorithms and security management.

Prototype 1 has been designed to verify interoperability with the real ICT environment. The planned next prototypes will be focused upon solving specific technology issues related to such particular implementations as using specific hardware, communication interfaces, or software environments.

4. Technology Description

a. Global Systematic Solution

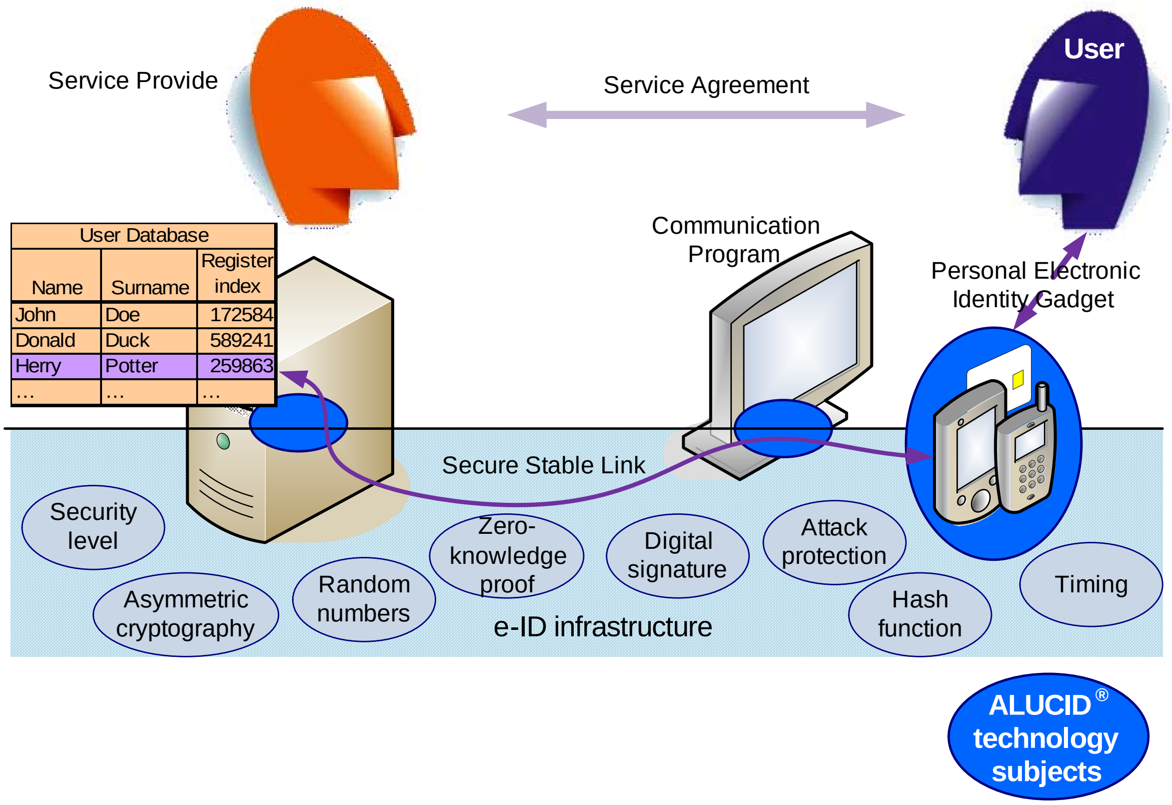
The basic principle of the designed solution is the transfer of all specific knowledge-demanding activities into the infrastructure. Experience from systematic design of other infrastructures has been used, and especially experience from the internet itself. Well-known, high-quality eID technologies and algorithms have been integrated and modified for the distributed seamless use by millions or even billions of mutually communicating systems.

- The infrastructure topology has been simplified. No intermediate subject, such as a certification authority or identity provider, is included. There are only the electronic service provider and the electronic service user.
- A personification of the eID device is not required. The identical eID devices can be produced without including any user-specific information. The eID devices are interchangeable with regard to their production and sale. The eID device creates an identity automatically by its own use in real life.
- No global identity, no global naming, and no naming authority are used. Identifiers are valid only between the user and service provider. The uniqueness of identifiers is solved automatically by the eID means itself, by the eID infrastructure. The only worldwide coordinated identifiers are those of the service provider. They are based on identifiers that are well-known and widely used on the internet, i.e. URI (DNS).
- No personal information is used in the eID infrastructure. Only pseudorandom numbers with temporary validity are carried over the public networks. No relation exists between the user's eID devices and the information carried over the network.
- The solution is not based on a single eID technology. Rather, it supports several authentication technologies simultaneously and is open for future enhancements.
- Full mesh topology is supported by design.

The systematic design is based on a simple abstraction. The eID infrastructure creates and supports a "secure stable link" between the user-owned eID device (the PEIG, or Personal Electronic Identity Gadget) and the item in the user database at the service provider's site. The link created and managed by the eID infrastructure is not dependent on the real identifiers and credentials used in communication over the network. Only the eID device supporting the link has the information connecting the real identifier and credentials with the link (see Figure 1).

The link is created automatically during the first connection to the service provider. The PEIG performs automatically all the activities needed to manage the user's eID. The user needs not to have any specific skills; the only thing he or she needs is to have the PEIG and to activate it.

The design supports a broad and flexible range of security levels. The length of identifiers and credentials can be changed within a wide range, and authentication levels can be selected together with the authentication method used, the algorithm and its parameters. Security management is supported by the eID infrastructure. The service provider is able to set up a minimal security level for its clients, and clients' PEIGs are able to acknowledge the level automatically if it is supported by PEIG implementation. The security level can range from a very basic level (comparable with RF-ID) to a very high level (comparable with PKI used for electronic signature or electronic citizen cards).



User Database

Name	Surname	Register index
John	Doe	172584
Donald	Duck	589241
Herry	Potter	259863
…	…	…

Figure 1: ALUCID Basic Abstraction

The design enables future improvements to the eID infrastructure without synchronisation of the users' and service providers' innovations. It enables changing the technology without severing the secure stable link. The service provider or user can upgrade his or her eID device without losing the link (the personified relation). The link can be transferred or cloned between two PEIGs owned by the same owner without copying of identifiers and credentials. The security level can be changed; the security algorithms used can be changed. New algorithms should be used without the loss of the link in future.

The design includes an integrated protection against network attacks. The protection has especially been improved at the client side of the infrastructure, where lies the weakest part of the current eID solutions. ALUCID uses well-known security systems like firewalls or proxies plus a new idea involving symmetrical authentication.

Open interface is included in the systematic design, as this is a well-proven method of interoperability support [3]. It should support seamless interoperability of different products from different suppliers in one eID infrastructure.

The design enables independent security auditing. The eID products and eID services should be independently verified and the result of verification will be easily accessible and understandable to the users. Together with the selling of empty eID devices without personification, this should simplify the end-user's life and enable selecting the right product on the market without any specific eID training or eID knowledge. Only standard market tools and methods are used.

e-Government specific point of view was described in [4].

b. eID infrastructure Supplier Point of View

Each supplier can place its own product or service onto the market, and it does not need to produce the entire infrastructure. Suppliers can find their own places position on the market and produce compatible products with specific features for their customers. A supplier can focus on the end-users and produce its own implementations of the PEIG with specific forms and features respecting the interoperability standards and security limits.

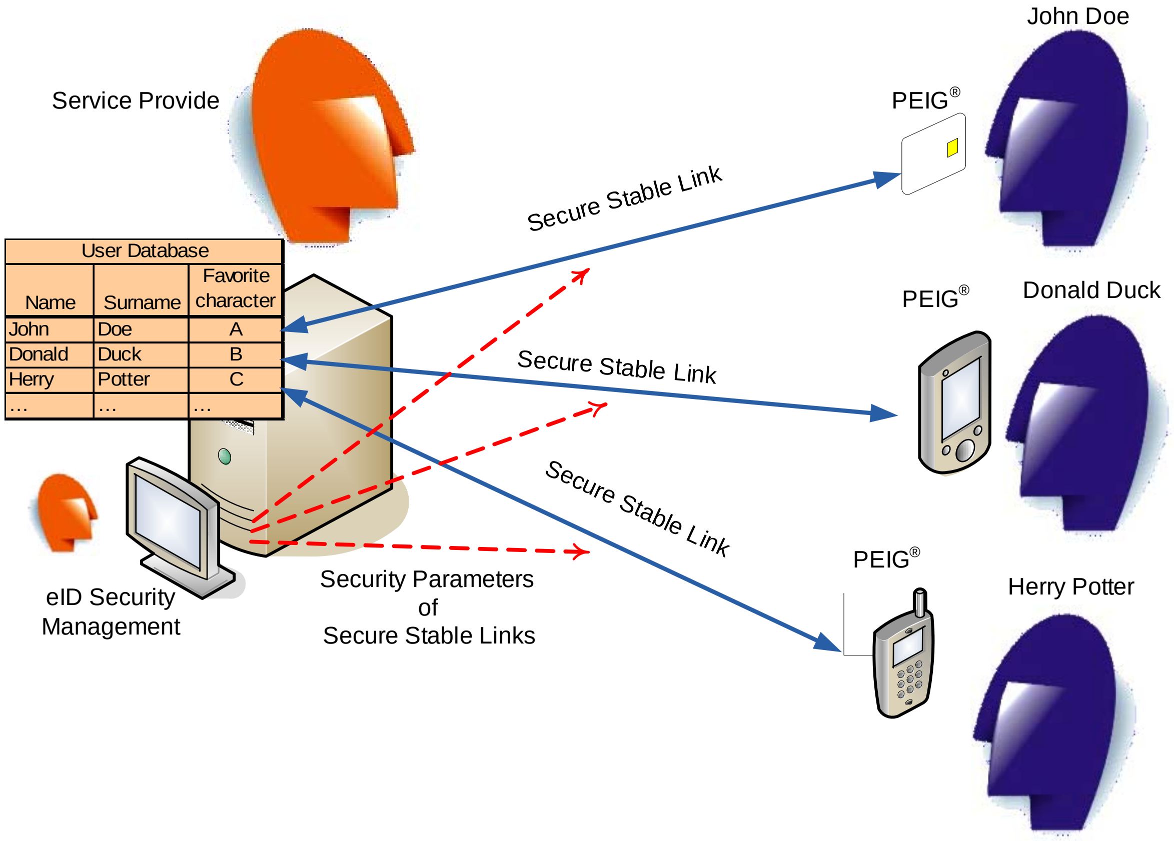
A supplier can also focus on the service providers and offer its own implementation of the ALUCID server component that is included or related to a specific ICT environment, such as a specific web server or portal. The supplier can focus on specific applications support, on certain services, or on outsourcing for service providers.

The eID infrastructure supplier should be familiar with all related topics of the eID infrastructure, including interface standards, protocols, security levels, security profiles, supported algorithms and methods, eID creation, updating, access control to identity data, timing, sequencing, and others.

c. *Service Provider Point of View*

The service provider's priority is its own service provision. The eID infrastructure can be used in a very simple way from that provider's viewpoint. The service provider buys the product or service from an eID infrastructure supplier and integrates it into its own service implementation.

The eID infrastructure will create and enable security management for the links between the service provider's user database and the users of its service. Identifiers and secrets will be managed automatically by the eID infrastructure with respect of the security parameters set up by the service provider's security manager.



User Database		
Name	Surname	Favorite character
John	Doe	A
Donald	Duck	B
Herry	Potter	C
…	…	…

Figure 2: Service Provider Point of View

From a service provider's viewpoint, all its customers are connected through the eID infrastructure directly and independently of other service providers. The service provider is virtually at the centre of all its customers. To the service provider, it looks like virtually no other service provider is connected to the eID infrastructure (see Figure 2).

d. End-User Point of View

The end-user's viewpoint is simple. It is user centric. The user buys one or more PEIGs, as he or she likes. It is his or her free decision. Maybe the form, colour, weight or other parameters are important for him or her. Perhaps the range of security levels supported by the PEIG, the PEIG's activation security, or the certification of the PEIG is important to the user. Then he or she teaches the PEIG to recognise him or her (secure activation of the PEIG), and the PEIG is prepared for use with a variety of service providers.

From the end-user's perspective, he or she is at the centre between all of his or her service providers. The PEIG enables him or her directly to communicate with the personified services. One click suffices to open the service of any of his or her service providers. To the end-user, it looks like virtually no other user is connected to the service providers (see Figure 3). Virtually only his or her personified services are provided by his or her service providers.

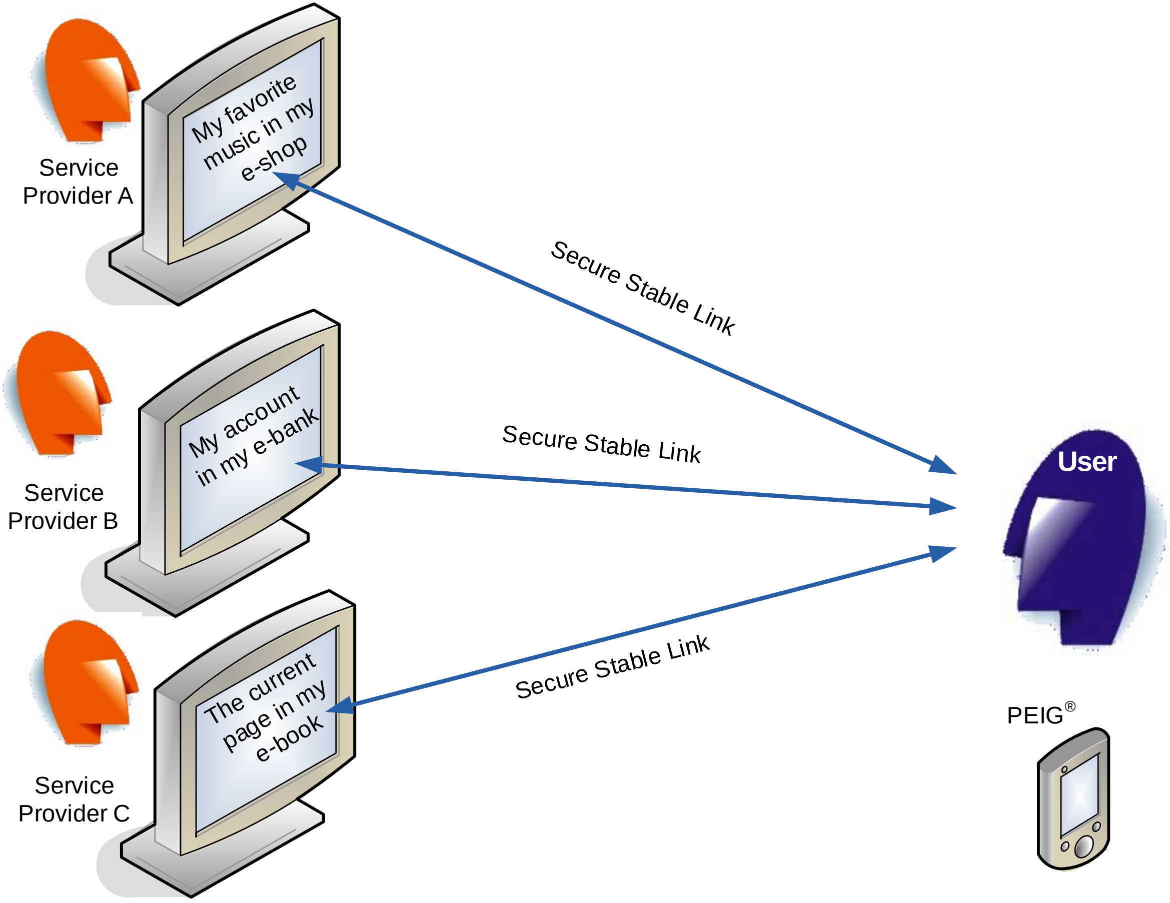


Figure 3: User Point of View

The end-user scenario should be as follows:

1. The user selects a PEIG he or she likes in a shop. It is sold empty. Anybody can buy it.
2. The user teaches his or her PEIG to recognise them when activated. Nobody else knows the activation information. The activation information is not used as any part of the eID.
3. The user connects the first time to the service provider and uses the activated PEIG. The PEIG automatically creates an eID for the user (together with the service provider system's eID means).
4. The user can (but need not) give their personal data to the service provider, and the service provider eID means are able to link this with user eID in a trustworthy manner.

5. The user will be able to open his or her personified service directly if he or she activates his or her PEIG. No login and no authentication process will be seen. It will be done automatically by the PEIG.
6. The same procedure (points 3–5) can be used with any other service provider supporting ALUCID. The number of service providers supported by the PEIG is limited only by the PEIG's internal memory size.

5. Developments and Results

The ALUCID design has been verified by models and prototypes.

The full range of system functions (e.g. anonymous identity; secure stable link; relation of identity with personal data; fully automatic identity generation; dynamic identity change; sharing of personal data without sharing of eID; one-time identity; data transfers between PEIG, user terminal, and service provider system) was verified in Model 1. The model did not include any real security algorithm. Model 1 was written in Visual Basic for Application [5] in the Microsoft Excel environment.

Model 1 enabled verification of all basic system design ideas and verified the limits of the architecture. The design was then slightly modified with respect of testing.

Security support was implemented in Model 2. The full support of real identities – including random numbers generation, real hash and cryptography algorithms – were used. Model 2 was written in Java [6] using standard Java Cryptography Architecture API [7].

Model 2 enabled verifying security levels, multiple authentication algorithm support, change of security level without loss of identity, use of security profiles, and basic security management. The design was then improved in the area of security management and in the interface description areas as a result of Model 2 development and testing. The first version of the ALUCID interface was then described (using XML/XSD).

Prototype 1 implemented the modified Model 2 in a real web environment. The service provider and the client site were implemented using standard http communication. A standard web browser was used as the user's communication program. The Tomcat [8] was used for implementing the service provider and client sites for ALUCID and for the testing applications. Prototype 1 included the first implementation of the PEIG. The PEIG was implemented in the standard USB flash memory.

The prototype 1 scope has been selected to minimise risks of implementation. The prototype has been implemented as a standard Web Service [9]. The verification was successful. The basic functionality was thereby verified in a real-life environment. The second version of the ALUCID interface was described as a result of the Prototype 1 implementation, and the http communication was slightly modified (simplified).

No significant implementation problem has been met. The objectives described in six eID common needs in [1] were reached at a prototype level. The limited network attack protection and set of e-government support functionality was included in the prototype

New prototypes are being prepared. The implementation of PEIG into mobile (cell) telephone is already prepared. Planned, too, is implementation of the more complex functions like "Identity Link" to support "remote heritage of PEIG introduction" in a real network environment or "Identity Clone" to support migration or copy of the secure stable link between PEIGs of the same user.

6. Business Benefits

If ALUCID will be successful, it can create an anonymous eID infrastructure where the idea of "A single European information space" [10] can be put into practice. The ordinary user should be able to simply and securely communicate with dozens or even hundreds of his or her personified services. The service providers should be able to manage in a productive and secure way the security of their customers. This could open possibilities for new personified electronic services in many areas. A “virtually private internet” should be created for every end-user. As a consequence, personal data protection could be significantly improved. Personal data could be placed only in secured information systems where the access can be managed. No personal data would be used where no access control could be made, namely in eID systems [4].

7. Conclusions

ALUCID is the outcome of a systematic design of a new eID infrastructure. It aspires to address all existing requirements for an absolute majority of participants in the real environment of today’s public networks, and especially the internet.

The solution has been simplified as much as possible to respect real needs and the real skills of the stakeholders.

The design has been verified successfully by the first models and prototype. More advanced testing and verification in pilots is needed to prepare the solution for real-life use.

Many challenges are still ahead, like real standardization of interfaces, deployment strategy, cooperation with market leaders, reaching of critical mass and they should be solved in future. We want to be open and co-operative, we look for partners.

References

[1] Neumann, L. “An Analysis of E-identity Organisational and Technological Solutions within a Single European Information Space”, *e-Challenges e-2007*, The Hague, Netherlands, 2007, pp. 1326–1333.

[2] Neumann, L., Sekanina, P. “Distributed Authentication and Authorization in e-Government”. *Conference Proceedings, 5th European Conference on E-Government*, University of Antwerp, Belgium, 2005, pp. 597–606.

[3] Neumann, L. “Strategic Options for Pan-European E-Government Interoperability”, *e-Challenges e-2006*, Barcelona, Spain, 2006, pp. 333–340.

[4] Neumann, L. “Anonymous, Liberal and User-Centric Electronic Identity Supports Citizen Privacy Protection in e-Government”. *Conference Proceedings, 8th European Conference on e-Government*, Ecole Polytechnique, Lausanne, Switzerland 10-11 July 2008.

[5] Microsoft, *Visual Basic for Application*, [online], Available: http://msdn2.microsoft.com/cs-cz/isv/bb190538(en-us).aspx [18 April 2008].

[6] Sun Microsystems, The *Java™ Tutorials*, [online], 14 March 2008, Available: http://java.sun.com/docs/books/tutorial/ [18 April 2008].

[7] Sun Microsystems, *Java™ Cryptography Architecture API Specification & Reference*, [online], 25 July 2004, Available: http://java.sun.com/j2se/1.5.0/docs/guide/security/CryptoSpec.html [18 April 2008].

[8] Apache, *Apache Tomcat*, [online], Available: http://tomcat.apache.org/ [18 April 2008].

[9] W3C, *Web Services Architecture*, [online], Available:http://www.w3.org/TR/ws-arch/ [23 Jun 2008].

[10] Commission of the European Communities (2006), *i2010 e-Government Action Plan: Accelerating e-Government in Europe for the Benefits of All*, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of Regions, Brussels 25.04.2006, COM(2006) 173 final, pp. 8–9.