THE ROLE OF ELECTRONIC IDENTITY IN THE INFORMATIZATION OF PUBLIC ADMINISTRATION AND SOCIETY

Буцко Й.
Вейачка М.

Информатизация общества является долгосрочной целью правительства Словацкой республики. В основе этой цели лежат развитие и выполнение обязательств, которые вытекают из проекта eEurope+, который определил странам-кандидатам на вступление в Евросоюз главные цели, направленные на ускорение реформы и модернизацию экономик путем внедрения и эффективного использования Интернета и информационных технологий. Одним из приоритетов этой деятельности является стимуляция использования Интернета, а именно путем ускоренного внедрения электронной коммерции, создание онлайн системы государственного управления, создание онлайн системы здравоохранения и т.п. В этой статье рассматривается проблема создания онлайн системы государственного управления как ключевого фактора информатизации общества.

Ключові слова: *державне управління, електронний зв'язок, інформатизація, електронна ідентичність, електронний підпис, е-Європа +.*

INTRODUCTION

The aim of this paper is to highlight the necessity of electronic citizen identity creation and its integration with the electronic services of public administration. This integration is the basis for more efficient use of electronic signature in Slovakia, which is a necessary step towards the computerization of public administration and informatization of society.

The basic document binding the states of the European Union to boost economic growth is the Lisbon Strategy adopted by the European Commission in 2000. The Lisbon strategy has become the basis for the emergence of other plans and strategies oriented at increasing the competitiveness of the EU and its members. One of the objectives of the strategy defined the need to build a knowledge-based economy as soon as possible. This objective inspired the creation of the action plan called eEurope, which continued in cooperation with more EU candidate countries as an action plan eEurope+ (Bucko, 2002, 111). The eEurope+ action plan was based on priority eEurope, but taken into account the specificities of each candidate states. The main objective of the plan was to accelerate the reform and modernization of the economies of candidate countries and improve their competitiveness (Bucko, 2002, 112). The starting point for the objectives set achievement was the requirement of effective communication between EU Member States development, what led to the need to build a unified information society. This led to addition of new target to eEurope+ plan. The content of this objective is to stimulate usage of the Internet in the following points (EU Commission, 2004):

a) Accelerating the e-commerce

b) Government online (electronic access to public services)

c) Health care online

d) European digital content for global networks

e) Intelligent Transportation Systems

f) Environment online

The main document, which aims at building a modern information society in Slovakia, the document "Information Society Strategy for the years 2009 - 2013" adopted by the Government on 21st October2009. The main goal of this document is to update the procedure for building the information society in Slovakia in respect of development and modernization of information and communication technologies and the emergence of new areas and directions of their use. The document defines key areas of society informatization and emphasizes their mutual relationship. One of the defined key areas becomes the issue of information security. Without a clear strategy of building information security is not possible to build a modern information society. The effective use of the Internet is closely related to the emergence of modern electronic services that are the basis of public administration computerization. One of the necessary conditions for the use of these services is the creation of user trust in these services (Mihók, Bucko, Delina, Paľová, 2008, 140). It is a complex process, which has several aspects, but a prerequisite of trust in electronic services (Bucko, 2010, 7) and progress to the computerization of government is to guarantee information security of these services.

The main document dealing with information security, the "National Strategy for Information Security of Slovak Republic", was approved by the Government by the 27th August 2008 (MOF, 2010). The document defines the three basic levels. The first level is a view of the strategic objectives of the Slovak Republic in information security in the long term, covering all important issues. The second level describes strategic priorities and in the third level are defined most important issues that serve as the basis for the key tasks achievement. The document contents also a basic description of each task to ensure the protection of the digital space of Slovakia in the range of unclassified information, mostly against information leaks, unauthorized use of information and disruption of data integrity.

From this perspective, the deployment and use of digital signature technology as the implementation of the legislative definition of an electronic signature is a must. From a technological point of view, digital signature satisfies all the conditions, and as a tool, it guarantees achieving information security. In conditions of Slovak legislative, electronic signature is equal with classic signature since 2002. Despite these facts, its use is lagging far behind expectations. The reasons are varied. One obstacle is ignorance and mistrust issues (including the creators of applications (Weinaug, Rabe, Mussina, Zanet, Azzopardi, Moksony, Mihók, Bucko, 2007, 15)), which is associated with low education level and awareness in this area. Another reason is the small number of applications using this technology and in particular the existence of simpler "non-electronic" alternatives. Changing this situation is essential to the task and computerization of public administration.

1 DESCRIPTION OF CURRENT SITUATION AND PROBLEMS OF ELECTRONIC COMMUNICATIONS WITH PUBLIC ADMINISTRATION IN SLOVAKIA

The central pillars of the dissemination of electronic signature are certification authorities, whose main function is to issue certificates to applicants. They stand in the center of Public Key Infrastructure (PKI), which provides electronic identity to citizens in a digital world and allow full electronic communication for the information society complying the strict rules of information security in an open environment such as the Internet.

The problem of electronic communication development in Slovakia and the general use of electronic identity is the tendency to use closed isolated systems. Qualified electronic signature has, despite of adequate Slovak legislation on e-signatures, general usage in open systems and should be accepted as full replacement for the traditional written signature in electronic communications with the public and other institutions in Slovakia, but the practice is different. Besides the fact of a small number of applications that allow its use, there is a tendency of closed systems. Institutions define their own terms of use of such communication that requires the use of a custom solution. This is usually based on the existence of the institution's certifying authority, which provides electronic identity accepted only in this closed system. Citizen gets into the situation, when he needs to create several electronic identities, what means increased costs, inconvenience and "electronic identity schizophrenia". The diversity of applications and user environments with the e-signature usage also contributes to its less frequent using. And if we compare these solutions with existing conventional options and their usage frequencies, motivation to use electronic signature application is very low.

Possibility of some improvements or even solution of this issue could bring the integration of electronic public administration services and institutions with the commercial sector, with usage of single electronic identity of the citizens supported by government initiative. Joint citizens' electronic identity would have become part of the solution and should be generally applicable in electronic communication with given institutions, which would create a single open system.

2 COMPARISON OF THE USE OF ELECTRONIC IDENTITY WITHIN THE EU

Within each of European Union member states the situation in the use of electronic signature and electronic identity is not the alike. The good indicator of the level of integration of PKI and electronic signature in the country is the measure of its e-Government services usage in the country.

The e-Government across the EU member countries uses for identification of entities various methods and technologies. In many countries is not an electronic signature (as the most suitable form of strong authentication) excessively wide-spread between end-users. The legislation in this area is within the EU good and harmonized in general. Commercial certification authorities issue an electronic signature for commercial purposes, but its acquisition is quite expensive. And if in the member country often is not sufficiently usable in praxis in different applications and in particular e-Government, its penetration between various subjects in given economy is low. Then there is less available for use in commercial applications, such as security in electronic banking and alike. This situation is common, especially in new member countries, including Slovakia.

In Slovakia, in the commercial sector now citizen can obtain a certificate from three commercial certification authorities at a cost of complex digital signature solutions from around 55 EUR, which is considerably higher price than in the most of other EU countries (D. CA Trust, 2009). For the purpose of use in its electronic banking only, electronic signature issued to clients of banks: VUB, Tatra banka and CSOB. Availability of electronic signature is so quite good, but if its usefulness in practice is low, so is its penetration. For individual subjects it is simply not enough usable and ineffective way to their identification at current price.

Based on experience from other EU countries it seems that the most appropriate way of introducing the electronic signature to the use by general population is issuing electronic identity cards (eID) linking functions Slovak ID card (identification in the physical world) with strong identification and authentication applications in e-Government. It increases penetration of electronic signature between the country's population significantly and thus creates an environment suitable not only for the development of e-Government applications, but also commercial applications.

The following table shows an overview of EU member states regarding the fact whether the state issues an electronic identity card to its citizens.

Table 1 Certification authorities in Slovakia

Providers of accredited certification service of qualified certificates management in Slovakia:		
Registration number	Name of ACA	Licenced since
ACA-003/2004	Prvá slovenská certifikačná autorita (PSCA)	15.06.2005
ACA-205/2006	První certifikační autorita, a.s.	21.09.2006
ACA-307/2007	Disig certifikačná autorita	26.07.2007
Certification authorities, which provide certified services only to selected government institutions in Slovakia:		
ACA-104/2005	Slovenská národná certifikačná autorita (SNCA)	15.8.2006
ACA-206/2006	Certifikačná autorita Ministerstva obrany SR (CAMOSR)	31.10.2006

Source: Bureau of National Security (NBU)

Table 2 Electronic identification card in EU states

EU State	ID Card with e-signature	Standard of data protection	Biometric data in electronic form	Use in e-banking	Other data stored on card	Use of ID card (since)
Belgium	yes	X.509	face	yes	health information	2003
Bulgaria	no	-	-	-	-	-
Cyprus	no	-	-	-	-	-
Czech republic	in plan	-	-	-	-	2012
Denmark	no	-	-	-	-	-
Estonia	yes	-	-	yes	health information	2003
Finland	yes	EAC	-	yes	social security	2004
France	no	-	-	-	-	-
Greece	no	-	-	-	-	-
Netherlands	no	-	-	-	-	-
Ireland	no	-	-	-	-	-
Lithuania	yes	EAC	face, fingerprints	yes	-	2009
Latvia	in plan	-	-	-	-	undetermined
Luxemburg	in plan	-	-	-	-	2012
Hungary	in plan	-	-	-	-	undetermined
Malta	in plan	-	-	-	-	undetermined
Germany	yes	EAC, PACE	face, fingerprints	yes	photo	2010
Poland	no	-	-	-	-	-
Portugal	yes	ELA 5	face, fingerprints	yes	-	2007
Austria	no	-	-	-	-	-
Romania	in plan	-	-	-	-	undetermined
Slovakia	in plan	-	-	-	-	2012
Slovenia	no	-	-	-	-	-
Spain	yes	EAC	face, fingerprints	yes	-	2006
Sweden	yes	BAC, EAC	face, fingerprints	yes	health information	2005
Italy	yes	X.509	face, fingerprints	yes	handwritten signature	2006
Great Britain	yes	BAC, EAC	face, fingerprints	no	-	2009

Source: own processing according to (EU Commission, 2010).

As the table shows, the situation in EU member states in electronic identity card implementing is not equal. Some countries do not have established obligation of ID cards for its citizens. Specifically the case of Great Britain, which introduced the eID on a voluntary basis, but new government, canceled this project and such licenses shall not be issued further. Resistance to this form of electronic identification introduction has historical roots in the resistance of the population of Anglo-Saxon countries (also in USA, Canada, Australia) against the identification card, which are not introduced there. In these countries, however, the e-government and e-signature applications are on significantly higher level than in Slovak conditions.

In countries that have introduced eID subsequently developed e-Government faster, as well as utilization of electronic signatures in commercial applications. Certification authority for eID is usually public or state administration institution in these countries and final price of eID cards for the end user is usually in the range of 10 to 30 euro. In many cases, eID card also stores additional information about the holder, such as biometric data (e.g. fingerprints), holder's medical records and so.

The best example of the introduction of eID to the praxis is Estonia - country that joined the EU at the same time as Slovakia. While in 2002 in Slovakia adopted the Law on Electronic Signatures, Estonia in January the same year issued the first such identification card - ID kaart, similar to our non-electronic identity card, but with a memory chip that stores secure electronic signature of cardholder. Within five years acquired their own electronic signature more than two thirds of all citizens of this country. Currently, the penetration of electronic signatures among the population of Estonia is over 90 percent level (at the age of legal eligibility). Root Certification Authority of Estonia (AS Sertifitseerimiskeskus) issues PKI certificates and Office for Citizenship and Migration issues identification card, while there are no fees for certificate, but for issuing the card Estonian citizen pays 24 EUR. The certificate is compatible with X.509 (Eesti Rahvusringhääling, 2010) standard.

As well as providing general services and e-Government services is this identification card used in banking, healthcare, education and commercial areas. In banking services is used (except for personal identification in physical locations) to authenticate transactions in electronic banking applications of nine banks operating in the country. Another important application of the Estonian ID card is its use as an electronic health cards, health records of citizens are transformed into electronic form and securely stored on the chip ID card of the person. In the education area it is mainly used in university applications such as university libraries, catering and so on. The eID card in the commercial area is mainly used in web applications and e-commerce by private companies. Finally let us mention the possibility of electronic elections in Estonia, which are also made possible because of secure electronic identification via electronic signature stored on the ID card of citizens. In municipal elections in 2009 approximately 15.75% of the all votes cast were voted via the Internet. It also enabled easier voting by citizens, who were abroad at the time of elections, and transmission of electronic votes was possible for 7 days and thus the through-time availability and convenience options were increased (ENEC, 2010).

Similarly, an electronic identity is resolved in Belgium, Finland, Lithuania, Germany, Portugal, Spain, Sweden and Italy, while in no country has yet been reported successful abuse of electronic identification by eID, suggesting high security of this solution. To introduce such a solution the electronic signature in the near future is planned in Czech Republic, Latvia, Luxembourg, Hungary, Malta, Romania and finally Slovakia. The remaining countries still do not intend to issue the eID. For Slovakia, the introduction of electronic identification card appears as a very suitable solution. Traditionally we identify people through ID card and thus next step could be extension of its functionality to the electronic space. Effectively usable e-Government applications are quite a few in Slovak public and state administrations and this could greatly enhance its usability, allowing unifying the identification in the various applications. We can also expect the development of many commercial applications due to the increased availability of strong authentication and authorization in the form of eID (EU Commission, 2010), (De Cock, Wolf, Prenet, 2008).

From this perspective it is good that the project is to introduce an electronic identity card in the SR was launched in June 2010. The implementer is Hewlett Packard Slovakia, Ltd., and it should last two years. This project is conducted by the Operational Programme Information Society (MVSR, 2009). Reasonable is the possibility of imposing medical information on eID and chip integration of payment services. The question is, why new identity cards were issued right after joining the EU without the implementation of electronic identification, and in that time, several member and candidate countries have already issued eID with electronic signature. Therefore development of e-government was slowed by years in Slovakia. Also it is questionable that how quickly will commercial sector will accept and benefit from the possibility of strong authentication and identification in their applications brought by the introduction of eID in Slovakia. In addition, expansion of electronic identity cards among citizens of the SR will only be gradual and progressive, because the exchange of old ID cards will take place after their gradual expiration.

On the other hand, thanks to a later introduction of eID in our country it is possible to benefit from the experience from its introduction in other countries. The most important experiences are:

- The need to overcome barriers to the use of eID in an electronic environment (lack of card readers, software bugs)
- The need for flexible design (possible subsequent additions of new functionalities)
- The need for removal of ignorance about how to use eID in an electronic environment (often eID holders perceived only as a physical document without electronic identification)

- The need for harmonization of various e-Government systems and services
- The need to overcome habits to use (less secure) already used forms of authentication in electronic banking
- Maximizing the availability of eID for citizens (low fees, issuing at many places, maximizing the availability of card readers)
- Broad support for alternative platforms (e.g. Linux) (Martens, 2007).

An important aspect of eID implementation in EU countries is the need to harmonize electronic identification systems in different countries and ensure their interoperability on an international basis.

CONCLUSIONS

The important trend in the use of electronic signature is facilitation of interoperability between applications that require strong identification in individual EU member countries. For example Belgian, Austrian, Estonian, Finnish and the Italian certificates issued and distributed through ID cards are interoperable with each other. There is the UES initiative (Universal Electronic Signature - Universal electronic signature), which aims to replace the handwritten signature by the electronic signature and is directed to allow international interoperability of electronic signatures within the EU (Martens, 2006). Implementation of UES initiative requires the following components to be adapted to the principles of universal electronic signature:

- Legislation
- Provision of certificate authority certificates on the device for secure generation and storage of certificates (SSCD)
- Verification process (verify the validity of the certificate in real time - OCSP)
- Tools for end users
- Cooperation between PKIs of member countries (Martens, 2006).

In harmonizing these aspects of the implementation of electronic signature is the objective of interoperability of electronic signatures in the EU achievable.

Another important trend in this area is the introduction of mobile electronic identity (e.g. functioning in Finland, Estonia). This technology integrates the electronic signature option into mobile phone SIM card. This technology enables to identify person and authenticate documents by electronic signature virtually anywhere. In Estonia nearly half of the applications using eID card also supports the use of such mobile identification (ID-Mobile Initiative, 2010).

BIBLIOGRAPHY

1. Bucko J.: eEurope+ a vzdelávanie manažérov na Slovensku. In: The 2nd International Conference on Applied Mathematics and Informatics at Universities 2002: Proceedings of Contributed Papers. - September 13. - 2002, Trnava, Slovak Republic. Trnava : Faculty of Material Science, 2002. - p. 109-114. ISBN 80-227-1752-5.
2. European commission - eEurope+ - Progress report 2004, European Ministerial Conference on the Information Society „New opportunities for Growth in a Enlarged Europe", Budapest, 26-27 February 2004, [cit 2010-11-01]. Available at: http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/benchmarking/eeuropeplus_progress_report.pdf.
3. Mihók P., Bucko J., Delina R., Paľová D. Trust and security in collaborative environments. In: Enterprise Interoperability 3: New challenges and industrial approaches. London: Springer Verlag, 2008. p. 135-143. ISBN 978-1-84800-220-3.
4. Bucko J. Dôvera a bezpečnosť na webových platformách, Habilitation thesis, 2010.
5. Ministry of finance of the Slovak republic- Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, [cit 2010-10-25]. Available at: http://www.finance.gov.sk/Default.aspx?CatID=6768
6. Weinaug H., Rabe M., Mussini B., Zanet M., Azzopardi J., Moksony R., Mihók P., Bucko J. Deliverable D08, Analysis and Prioritization. FP6 IST Strep Project N° FP6-027 083, FLUID-WIN, 2007.
7. Trust certification autority: Cenník produktov a služieb. [online]. Bratislava. 2009. [cit. 2010-10-11]. Available at: http://www.dtca.sk/services/pricelist.php
8. European commission: State of play concerning the electronic indetity cards in EU Member States. [online]. Brussels. Belgium. 2010. [cit. 2010-10-12]. Available at: http://www.statewatch.org/news/2010/sep/eu-council-national-id-cards-13152-10.pdf
9. Eesti rahvusringhääling: National ID Card Fee to Rise Next Year. [online]. ERR News. Tallinn. Estonia. 2010. [cit. 2010-10-10]. Available at: http://news.err.ee/f3f6abe5-13b9-4beb-bf84-dc5331578263
10. Estonian national electoral committee: Internet Voting in Estonia. [online]. Tallinn. Estonia. 2010. [cit. 2010-10-09]. Available at: http://www.vvk.ee/index.php?id=11178
11. De cock D., Wolf Ch., Preneel B. The Belgian Electronic Identity Card (Overview). [online]. Brussels. Belgium. 2008. [cit. 2010-10-12]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.2793&rep=rep1&type=pdf
12. Ministry of interior of the Slovak republic: Národný projekt: Elektronická identifikačná karta. [online]. Bratislava. 2009. [cit. 2010-10-11]. Available at: http://www.minv.sk/?EID_MV
13. Martens T. Estonia - The Country with Identification Infrastructure. [online]. Tallinn, Estonia. 2007. [cit. 2010-10-08]. Available at: http://siteresources.worldbank.org/EXTEDEVELOPMENT/Resources/Martens_Estonia.ppt
14. MartensT. Universal Electronic Singatures. [online]. Tallinn. Estonia. 2006. [cit. 2010-10-08]. Available at: http://www.openxades.org/ues/UES.ppt
15. Mobil-id initiative: Personal Identification and Authentification with a Mobile Telephone. [online]. Tallinn. Estonia. 2008. [cit. 2010-10-10]. Available at: http://www.id.ee/?id=10995&&langchange=1