eXclusive e-JOURNAL
ISSN 1339-4509

ECONOMY & SOCIETY & ENVIRONMENT

Digital certificates for public services

Tomáš Bálint, Jozef Bucko, Martin Vejačka

Department of Applied Mathematics and Business Informatics,
Faculty of Economics, Technical University of Košice
Nemcovej 32, 04001 Košice
tomas.balint@tuke.sk, jozef.bucko@tuke.sk, martin.vejacka@tuke.sk

Abstract The electronic communication in public administration is of major importance in the last years. New services such as e-procurement, e-auctions, and digital communication in general need efficient ways to secure data exchange. Digital certificates, together with certificate authority (CA) represent core components of the public key infrastructure (PKI) which can be used to secure digital identity. To deploy this infrastructure, multiple software tools, both commercial and open-source, are available. The paper presents fundamental issues and challenges in this field. Reference certificate authority solution deployed in academic environment is characterized. The core contribution of the paper is a proposal of new indicators which can be used to assess efficiency of PKI deployment in public sector.

Key words Certificate authority, digital certificates, e-government, public key infrastructure, public services

1. INTRODUCTION

Public administration and public services in general in recent years face new challenges when introducing electronic communication and informatization, respectively transformation of its processes into the electronic environment. Very important challenge, especially in the areas of e-procurement and e-auctions (Prídavok et al., 2013), is the identification in the electronic environment and trust-building within this environment (Delina et al., 2012). Nowadays, electronic communication is reality. Electronic documents' interchange accelerates business processes, data processing and other documents is more comfortable, reduces the error rate and improves the archiving possibilities. Electronic documents interchange through electronic mail or web portal is reliable and sufficient if the transmitted documents do not contain sensitive information. However important content can be misused or modified, when transferred through email or web. The reason is openness and low security of the Internet. In this case, it is necessary to use the classic form of communication and documents delivered in person or authorize by a notary service and use standard mail or courier services.

The analogy to the classical signature that authorizes the document and allows the electronic documents interchange and electronic communication is electronic signature based on asymmetric encryption technology. Digital signature technology enables efficient authorization of the document contents and prevention of change. Further it allows concealing the document content if it is required. Compared with the classical signature is the use of this technology safer. Also if all the requirements under the Act on electronic signature (which is valid in Slovakia since 2002) are met, then it is equal sign with a classic handwritten signature. When speaking about "open system", the validity of electronic signature is

general and it should be accepted by all Slovak public institutions and subjects. Successful and active use of electronic signatures in open systems requires a well-developed and functioning infrastructure and legislative support in the form of act on electronic signature.

Deployment of electronic signatures is possible in an environment with limited validity, aimed at a particular application in specific cases and infrastructure (so-called "closed system"). In such environment, the validity of electronic signatures and the way of use is subject to internal rules of the system. The advantage is faster and easier deployment, higher control over the system and less complexity. There is a lot of such closed systems that use electronic signature, examples are banks (e.g. in Slovakia: VÚB, ČSOB, Tatrabanka etc.) or public institutions (e.g. Tax Directorate, Customs Office etc.).

The basis for the use of electronic signatures in any system is well functioning and all safety requirements fulfilling Public Key Infrastructure (PKI). The center of the PKI is Certificate Authority or Certification Authority (CA), which acts as a trusted independent party (electronic notary) and according to the law it issues, confirms and maintains a list of valid certificates of the system users.

In Slovakia, there are five accredited certification authorities (ACA), which are accredited to issue certificates to users, the validity of which is in accordance with the Law on electronic signature. In addition to ACAs there are a number of certification authorities (CA), which form the basis of closed systems with varying degrees of relevance and applicability.

2. SOFTWARE FOR DIGITAL CERTIFICATES

The aforementioned challenges of digital certificates' integration in everyday processes which are required by the public administration and government can be achieved only with the appropriate technical resources. The core component of every PKI infrastructure is the certification authority. From the technical point of view, CA is implemented as a complex piece of computer software with multiple modules and interfaces.

The portfolio of available software products for the PKI deployment is rather restricted. This is due to the fact that correct implementation of the PKI requires integration of a cryptographic module in the whole system. This module is an essential part of the whole PKI ecosystem because it performs the basic operations needed for digital certificates and digital signatures operations. Development and integration of such a module is costly and long-running process which increases significantly the fixed costs of PKI development.

Therefore, only a small number of software products for building public key infrastructure are available on the market. From the proprietary software group we can mention certificate authority which is available as a part of the Microsoft Server software. The other possibility is to build certificate authority for public services from available open-source solutions. This solution is particularly attractive in e-government environment where the question of costs is important. The open-source software can be modified to the needs of an organization. Among the available open-source solutions for the deployment PKI services we can cite gnoMint (gnoMint, 2013), OpenCA (OpenCA, 2013), and EJBCA (EJBCA, 2013).

The last mentioned solution, EJBCA, is an enterprise PKI CA which is built using Java programming language by the Swedish software engineering company called PrimeKey Solutions (EJBCA, 2013). The EJBCA is today available in two different versions: enterprise and community. The first is fully certified commercial version which complies with the current standards and international laws. On the other hand,

the community version is aimed on the customers who does not necessarily need fully certified version, compliant with security standards. This open-source CA is one of the most widely used PKI solutions in the world. Among the reference installations one can find French ministries of Defense and Finances, National Swedish Police Board, or Chinese Local Taxation Bureau of the ZhuHai city.

3. DEPLOYMENT OF PKI: REFERENCE INSTALLATION CAEKFTUKE

At the Faculty of Economics, Technical University of Košice there exists for multiple years research in the field of electronic signatures' deployment and their use in business and public services. Since 2010 there exists here a fully working installation of the EJBCA from PrimeKey Solutions. The acronym for this reference installation is CAEKFTUKE (Certificate Authority of the Faculty of Economics, Technical University of Košice) (CAEKFTUKE, 2013). This installation started as a Master thesis project of one of this paper authors. Nowadays, this certificate authority serves for three main purposes. In the first place, it is an experimental environment for the researchers in the Department of Applied Mathematics and Business Informatics. Secondly it is used in the educational process to demonstrate the creation, working operation and revocation of digital certificates for the students of two bachelor study programs. They use it not only for the experiments with digital signatures, but also for the signing of emails and work with electronic documents' registry of the faculty. The last function of this CA is to provide SSL certificates for the faculty servers. In this way employees and students can access faculty information systems, which are mainly web-based, through safe encrypted connection.

Figure 1: Homepage of the CAEKFTUKE

The deployment of complex PKI infrastructure needs an appropriate hardware and software tools. The current installation at the Faculty of Economics, TUKE is deployed on a server with 2 GHz Intel Xeon core and 8 GB of RAM. The system runs on Linux OS (Ubuntu) with JBoss 5.1. application server, Tomcat web server, and MySQL database.

4. MEASURES OF PKI EFFECTIVENESS

The construction of indicators is an effective way of systems' performance assessment (Janke et al., 2013). To facilitate the comparison and measurement of multiple Public Key Infrastructure solutions' usage in public services, we have decided to design a set of indicators to address various aspects of PKI solution introduction into practice use. They are defined and characterized hereafter.

Efficiency Indicator:

$$I_e = \frac{Number\ of\ users}{\sum PKI\ introduction\ costs}$$

Efficiency indicator gives in ratio number of users with sum of costs involved in PKI introduction. The higher I_e means better efficiency of costs spent on introducing of PKI in given public administration application.

Usage Intensity Indicator:

$$I_{UI} = \frac{Number\ of\ uses\ within\ half\ year}{Number\ of\ users}$$

Usage Intensity Indicator 2:

These indicators show the intensity of PKI solution use by giving number of uses within year (or half year) into ratio with number of users of given PKI. The higher number of uses by PKI users means higher intensity of PKI use. Comparison of both these indicators can show if speed of PKI adoption is increasing or decreasing. When I_{UI2} is higher than $2I_{UI}$, usage intensity of PKI solution is increasing in time.

Indicator of adoption:

$$I_a = \frac{Number\ of\ users\ to\ date}{Number\ of\ all\ potential\ users}$$

Speed of adoption indicator:

$$I_{a2} = Time\ until\ half\ of\ elegible\ users\ adopts\ use\ of\ PKI$$

Both these indicators show how fast is PKI solution adopted in given case of use. Higher number of users using PKI solution to date in context of all potential users in given country shows fast adoption of PKI. Indicator I_a a may have value from range <0, 1>.

Indicator of usability:

$$I_u = \frac{Number\ of\ services\ available\ by\ use\ of\ PKI\ solution}{Number\ of\ all\ public\ services}$$

For PKI use in public services is necessary to introduce wide palette of public administration applications to allow its use in multiple cases and increase its usability. Indicator of usability shows how widely the PKI solution is usable in terms of all public services available in given country. Indicator I_u may have value from range <0, 1>.

Indicator of security:

$$I_s = \frac{Number\ of\ misuses}{Number\ of\ uses}$$

This indicator shows ratio of number of misuses with number of users. The PKI solution is safer, when number of misuses lower at given quantity of users. Indicator I_s may have value from range <0, 1>. The lowest level of security indicator (I_s = 0), indicates that PKI service was never misused and is the most desirable value. The highest level of indicator of security (I_s = 1) would mean complete misusage of PKI solution every time it is used.

The nature of indicators of security, usability and adoption allows us to compose integrated indicator from these single indicators. It might have following form:

$$I_{PKI} = \frac{I_a + I_u}{2} - I_s$$

This composite indicator considers several aspects (usability, security and rate of adoption) of PKI use in public services and gives fast view of quality of PKI solution introduced in public administration of given country. Indicator I_{PKI} may acquire value from range <0, 1> and the highest value (0) represents ideal PKI introduction with full adoption ($I_a = 1$), usability of PKI for all services of public administration in country ($I_u = 1$) and maximum security with no misuses of given PKI solution ($I_s = 0$).

5. CONCLUSION

Public key infrastructure allows issuance of certificates digital signature. In this article we deal with the issue of the use of these digital certificates issued by certification authorities for the purposes of electronic communication when using various electronic services. PKI certificates can be issued by certification authorities with different software solutions. We further discussed open source solution of certification authority EJBCA from PrimeKey Solutions, which is in practical use in the educational process in the form of Certificate Authority of the Faculty of Economics, Technical University of Košice (CAEKFTUKE) at our faculty.

Furthermore, we propose several indicators to measure the effectiveness of PKI solutions and making it possible to compare several solutions among themselves. In addition, we proposed composite absolute indicator that shows basic quality of PKI solution in one absolute measure. Our further research will focus on the use of the proposed indicators to evaluate the effectiveness of multiple PKI solutions.

Acknowledgement

The research was realized within the national project “Security models of distributed systems providing electronic services” (Contract No. 1/0945/12) funded by Grant Agency for Science; Ministry of Education, Science, Research and Sport of the Slovak Republic.

References

1. Bačík, R., Fedorko, R., Fedorko, I. 2012. Internet marketing. Prešov : Bookman, 2012, 105 s. ISBN: 978-80-89568-64-2.

2. Bačík, R., & Fedorko, I. (2013). Komparácia systémov kontextovej reklamy PPC. eXclusive JOURNAL, 1(1), 91-98.
3. CAEKFTUKE – certificate authority of Faculty of Economics, Technical University of Košice - homepage. (2013). Cited [2013-05-02]. Available online at: https://v2.ekf.tuke.sk
4. Delina, R. Tkáč, M., & Janke, F. (2012). Trust building electronic services as a crucial self-regulation feature of Digital Business Ecosystems. Journal of Systems Integration, 3(2), 29-38.
5. EJBCA – Enterprise Java Beans Certificate Authority - homepage of software product (2013). PrimeKey Solutions, cited [2013-04-30]. Available online at: www.ejbca.org
6. gnoMint – X.509 Certification Authority management tool – homepage (2013). Cited [2013-04-30]. Available online at: http://gnomint.sourceforge.net/
7. Janke, F., & Prídavok, M. (2012). B2B network performance: practical aspects of network supply adequacy indicator. In: IDIMT-2012: ICT Support for Complex Systems : 20th Interdisciplinary Information Management Talks : Jindřichův Hradec, Sept. 12-14, 2012, Česká republika. - Linz : Trauner Verlag, 337-346. ISBN 978-3-99033-022-7
8. OpenCA – Opensource Security and Identity Management Solutions – homepage (2013). Cited [2013-04-30]. Available online at: www.openca.org
9. Prídavok, M., & Delina, R. (2013). Effective Spend management Through Electronic Reverse Auction Configurations. Quality Innovation Prosperity, 17(1), 1-9.