Electronic Business and PKI System of the Post Serbia

Dragan M. Spasić[1]

Abstract - **Public enterprise of PTT communications "Srbija" (Post Serbia) has decided to make the PKI system and establish the public Certification Authority. Therefore, new technologies such as e-commerce, e-banking and e-government demand protected Internet communication, and PKI system is the basis for the application of the most various mechanisms of electronic transaction protection. The services and digital certificates of PKI system and Certification Authority of the Post Serbia are intended for the internal use in the framework of the Post Serbia as well as for all the external participants of electronic business, regardless whether they are legal or natural persons.**

Keywords - **Public Key Infrastructure (PKI), Certification Authority (CA), digital certificates.**

I. INTRODUCTION

The success of electronic business depends completely on the protection of business transactions on Internet. As a matter of fact, Internet gives large possibilities in the field of electronic business, but on the other hand, creates problem of data protection. Among problems that appear, the following must be emphasized: unauthorized connection to the network, unauthorized access to network resources, revealing content of messages that are exchanged by network – problem of the secrecy of inventions, unauthorized modification of messages – problem of integrity of messages, forging the messages, forecast of the activities performed, etc. In order to prevent appearance of the problems mentioned, it is necessary to apply various mechanisms of protection, i.e. it is necessary to maintain the appropriate system of protection.

The existence of the Public Key Infrastructure – PKI system is the precondition for the successful conducting of various methods of protection of electronic business. Actually, PKI system is the basis for the application of various solutions of protection that are based on technology of symmetry and asymmetry cryptography systems and technology of digital (electronic) signature.

The solutions of protection of electronic business that are based on PKI system secure four (4) basic functions of protection:

1. Confidentiality – guarantees that the content of the message shall be revealed to the intended receiver of message only.
2. Authentication – verifies the identity of the user that communicates over the network.
3. Integrity – guarantees that the message has not been changed while transferred.
4. Nonrepudiation – does not allow the denial of the transaction performed.

The protection of the secrecy of the message (confidentiality) is enforces by encrypting the message by the application of the suitable cryptographic system, while the other three functions of protection are realized by the technology of digital signature.

II. COMPONENTS OF PKI SYSTEM

The most important components of the PKI system are the following:

1. Certification Authority (CA),
2. Registration Authority (RA),
3. Public directory,
4. User (client) applications.

Certification Authority performs the following activities:

- issuing, renewal, suspension and revoking of digital certificates,
- configuration of various types, life cycles or other parameter of certificates,
- renewal of CRL (Certificate Revocation List),
- cross-certification with other Certification Authority, and other.

Registration Authority represents a connection between the users that pass demands for issuing certificates and the Certification Authority. Tasks of the Registration Authority are the following:

- accepting demands of the users for issuing certificates,
- verifying identity of users and collecting the necessary data on the users,
- transfer of the demands of users for issuing certificates towards the Certification Authority, and other.

Public directory is the location where the Certification Authority publishes and keeps the following public data:

- Data on the users,
- Digital certificates,
- CRL (Certificate Revocation List).

User applications enable the users to take advantage of the digital certificates to perform protected on-line transactions.

[1]Dragan M. Spasić is with the Public enterprise of PTT communications "Srbija" (Post Serbia), Katićeva 14-18, 11000 Belgrade, SCG, E-mail: dspasic@ptt.yu

III. DIGITAL CERTIFICATES

Digital certificate is an electronic document that is issued by the Certification Authority. Digital certificate can be perceived as the digital personal identity card, since it contains the data on the user (owner) of the certificate and data on the publisher. It contains (Fig. 1.):

1. data on identity of the user to whom the certificate has been issued, such as the name and surname, e-mail address, etc,
2. public cryptographic key of the user of certificate,
3. data on the entity that has issued the certificate or the Certification Authority.

Within this framework of the digital certificate that is issued to the user, there is, among other, also the user's public cryptographic key, representing a pair to his private cryptographic key. Certification Authority guarantees accuracy of the data in the certificate, i.e. guarantees that the public key situated in the certificate belongs to the user whose data has been mentioned in the same certificate. Therefore, the other users on Internet, if they have confidence in the Certification Authority, can be sure that a certain public key really belongs to the user who is the owner of the private key. Digital certificate is impossible to forge, because it has been signed by the private key of the Certification Authority.

Digital certificate is electronic document that is publicly available on Internet. Therefore, in framework of certificates, there are public keys of the owner of certificate, and the distribution of certificate is also distribution of the public keys. For that reason, we have enabled the competent exchange of public keys by means of Internet between the users that have never met, with the possibility of verification of the identity of users.

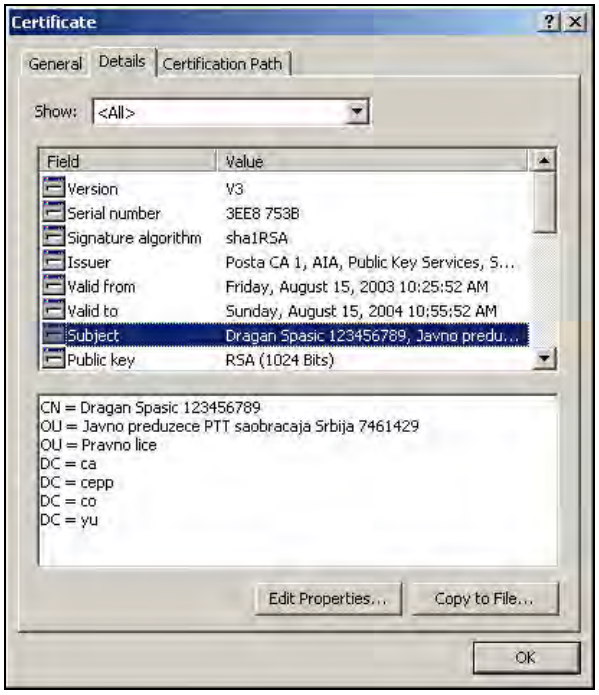

Fig. 1. Digital certificate, tab Details

IV. PKI SYSTEM AND CERTIFICATION AUTHORITY OF THE POST SERBIA

The Post Serbia has decided to make the PKI system and establish the public Certification Authority (CA). Therefore, new technologies such as e-commerce, e-banking and e-government demand protected Internet communication, and PKI system is the basis for the application of the most various mechanisms of electronic transaction protection.

PKI system of the Post Serbia has been made in accordance with the Entrust technology [1]. Company Entrust is world acknowledged producer of PKI solutions, that, in accordance with the realized PKI systems, is dominant in the world.

PKI Post Serbia system has hierarchical organization (Fig. 2.). In the first phase of production of PKI system, there are installed two CA servers:

- Root CA server ("Posta CA Root"),
- Issuing CA server ("Posta CA 1").

In the second phase, Post Serbia have planned to install two more servers:

- Issuing server ("Posta CA 2"),
- Timestamp server ("Posta TS").

Hierarchical organization of the PKI Post system consist of the two levels of CA server (Fig. 2.), that are placed in the relation of superior - subordinate CA servers. Such organization of PKI system with the greater number of CA servers enables: increased availability of PKI services (if one CA server fails, the others are available), flexible organization of PKI services, distribution of administrative authorities and duties, application of the various forms of protection in accordance to levels.

Root CA server is in the off-line regime of operations. This minimizes the risk of compromising the root CA private key. However, private key of the root of CA server is the most critical element of the entire PKI system. Apart from that, there are all measures taken in order to keep the private keys, of the issuing CA servers that work in the on-line regime, remain secret. The protection of CA servers is executed by the application of the following measures of protection:

1. Physical security,
2. Protection of communications,
3. Protection on the level of operation system and communications,
4. Organizational measures of protection.

Apart from the CA servers, PKI system of the Post Serbia consists also of the following servers and administrative workstations.

- Main Directory server where the Master Directory Service pertains.
- Public Server where a copy of the Public Directory is situated – Shadow Directory Server.

- Web server with the application for the reception of the requests of the Registration Authorities for the issue of certificates.
- Web server with the application (Entrust Web Connector) for the issue of certificates to the users through Internet.
- Workstations for the administration of CA servers and the issue of certificates.
- Workstations for the supervision and configuration of firewalls.

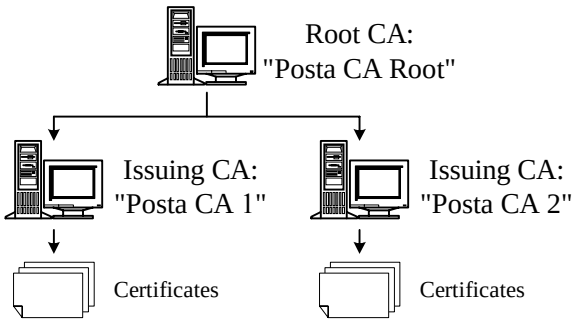

Fig. 2. Hierarchical organization of CA servers in the Post Serbia

V. Digital Certificate of the Post Serbia Certification Authority

PKI system of the Post Serbia is the commercial PKI system that shall, after being released into production, offer to the interested buyers the services of the issuing of the digital certificates. Certification Authority of the Post Serbia has at the disposal the following four (4) types of certificates [2-4]:

1. Entrust Enterprise certificate for more applications (Multiple application ID),
2. Entrust Enterprise certificate for one application (Single application ID).
3. Web certificate.
4. Certificate for Web server.

Entrust Enterprise certificates are standard X.509 version 3 certificates that have been adjusted to the Entrust applications, and they can be used also by the "Entrust-Ready" applications. There are two (2) types of the Entrust Enterprise certificates:

1. Enterprise certificate for more applications (MID). The user with this certificate can obtain the client application Entrust Entelligence and the possibility of using certificates with the unlimited number of applications and plug-ins.
2. Enterprise certificate for one application (SID). The user with this certificate obtains the client application Entrust Entelligence and the possibility of using the certificates with only one application or plug-in.

Client application Entrust Entelligence is delivered with every Entrust Enterprise certificate and it enables the following:

- Obtain and renewal of Entrust Enterprise certificate, survey of content of certificates and exporting of certificates in the files of the various formats (Public Encryption Certificates for Entrust Users – file .key, Public Encryption Certificate for S/MIME Users - file .p7c, Certificates and Keys using the PKCS#12 – file p.12).
- Encrypting / decrypting files and signing /verification of the signed files (Fig. 3.).

Considering the fact that there is a compatibility with Microsoft CryptoAPI, it has been enabled to use Entrust Enterprise certificates in the framework of the Microsoft applications (Internet Explorer, Outlook, Outlook Express, Word,...), as well as applications of the other vendors. Microsoft applications are using Entrust Enterprise certificate through Microsoft CryptoAPI interface that is completely transparent for end users.

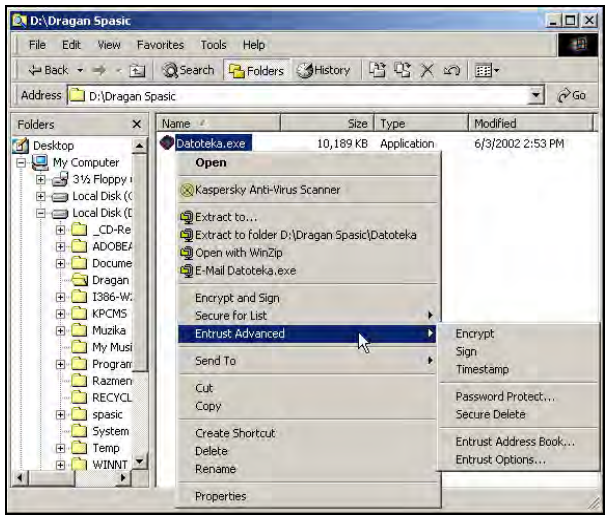

Fig. 3. Options of client application Entrust Entelligence

Web certificates are standard X.509 version 3 certificates that can be used in the framework of Microsoft applications (Internet Explorer, Outlook, Outlook Express, Word,…) and applications of other vendors. Apart from that, Certification Authority of the Post Serbia can be adjusted to the Web certificate in accordance to the demands of the users (applicants) of the certificate. For example, Certification Authority of the Post Serbia can adjust the Web certificate for the needs of the bank that intends, in process of electronic banking, to implement utilization of certificate, and in such a way, secure the protected communication.

Web administrator can install certificate for Web server on Web server, configure Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) protocol and provide confidential communication between Web server and clients [5].

Apart from the certification, the Post Serbia is able to offer to the interested users also plug-ins for the Entrust Enterprise certificates:

1. File plug-in titled Entrust ICE. It enables the creation of folders where the files are automatically encrypted after the copying in that folder (Fig. 4.).

2. E-mail plug-in titled Entrust Express. After the installation, it has been completely integrated in the framework of E-mail client application Microsoft Outlook (Fig. 5.) and it enables the encrypting / decrypting and signing / verification of signed e-mails.

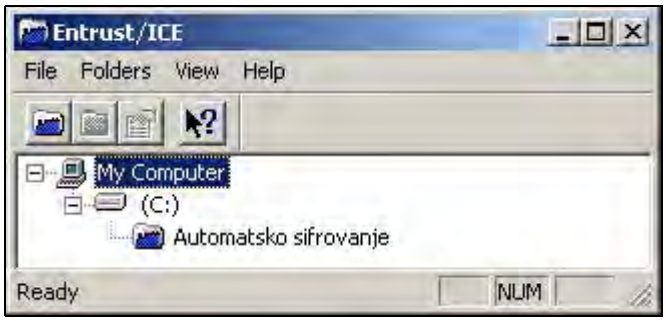

Fig. 4. File plug-in Entrust ICE

Fig. 5. Options of the E-mail plug-in Entrust Express

VI. Protection of On-Line Transactions

Post Serbia plans to offer to the potential users applications and solutions which by using digital certificates enable the protected on-line communication:

- Signing and encrypting of transactions of e-banking and e-commerce that are exchanged by Internet.
- Protected E-mail communication.
- Protected Web communication.
- Log in on the computer, computer network or application.
- Signing code of software packages.
- Signing and encrypting of files, either to store them on hard-discs of the computer or to exchange them by computer network.

VII. Potential Users

The most important potential users of the Post Serbia certificates and applications are the following:

- Post Serbia (internal user),
- Banks and other financial institutions.

Apart from the mentioned most important potential users of the Post Serbia certificates and applications, the Post takes care of the needs for the certificates and other potential users:

- Internet providers,
- Providers of e-banking,
- Providers of e-commerce,
- Providers of telecommunication services,
- Government institutions,
- Individual users.

VIII. Conclusion

Post Serbia pretends to become the first public Certification Authority in the Republic of Serbia that shall issue the digital certificates to the participants in electronic business (institutions, organizations, companies and individuals). The services of PKI system and Certification Authority of the Post Serbia are intended for the internal use in the framework of the Post as well as for all the external participants of electronic business, regardless whether they are legal or natural persons.

Difficulty in becoming public Certification Authority in the Republic of Serbia is the lack of the Law on Electronic Signature. That law should be introduced to establish the use of electronic signature in administrative, judicial and other procedures, business and other actions, as well as rights, obligations and responsibilities with regard to the digital certificates.

References

[1] Entrust Web site: http://www.entrust.com.
[2] "Entrust Authority Security Manager Comprehensive", Entrust Technologies, 2002.
[3] D. Spasić, "Digital Certificates of the Post Certification Authority", X Conference "YU Info 2004", Conference Proceedings (CD-ROM), Kopaonik, SCG, march 2004.
[4] D. Spasić, "Obtaining Entrust Digital Certificates", IV Conference "E-trgovina 2004", Conference Proceedings (CD-ROM), Palić, SCG, april 2004.
[5] D. Spasić, "Secure Web Communication and Digital Certificates", VIII Conference "JISA 2003", Conference Proceedings (CD-ROM), Herceg Novi, SCG, june 2003.
[6] D. Spasić, "Cryptosystems and Digital Certificates", IX Conference "YU Info 2003", Conference Proceedings (CD-ROM), Kopaonik, SCG, march 2003.
[7] "Microsoft Windows 2000 Server Resource Kit", Microsoft Corporation, 2000.
[8] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.
[9] "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures", Official Journal of the European Communities, L 13/12, 19.1.2000.