ISSN 0354-9852
DOI 10.7251/AKT3215002N

UDK 004.056.55:004.738.5
Pregledni rad/Overview paper

PKI SYSTEMS, DIRECTIVES, STANDARDS AND NATIONAL LEGISLATION

Nikola Novaković[1], Milan Latinović[2]

Abstract

This paper describes Public Key Infrastructure (PKI). It is a platform for the realization of secure methods of information exchange based on public key cryptography. The introduction of these systems implies knowledge of the directives and standards prescribed by the organization for the introduction and improvement of standards. Similarly, the introduction of PKI system must meet the legal requirements prescribed by national legislation. This paper presents a list of organizations and standards related to PKI systems, and analysis of domestic legislation which is necessary to know prior to the realization of any specific methodology or implementation. The aim of this paper is an introduction to the problems of PKI systems and view at the basic regulations (directives, standards and legislation), whose knowledge is a prerequisite for the concrete implementation of these systems.

Key words: *Public Key Infrastructure (PKI), key cryptography, basic regulations*

JEL classification:C8

INTRODUCTION

With the development of information and communication technologies (ICT) new modern IT societies started to appear based on usage and exchange of information strictly in electronic form. One of the steps that every informatics society must pass through (in order to get the title informatics society) is transformation of the administration to fully electronic administration. In order to make it possible, it is necessary to provide mechanism of electronic documents exchange that guarantee authenticity of electronic documents, that is, it is necessary to find the mechanism that stands for signature and seal, that are proof of authenticity and mechanism for determination of document's issuer identity in paper administration

1 MA Nikola Novaković, Banjaluka College, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, nikola.novakovic@blc.edu.ba

2 MA Milan Latinović, Agency for Information Society of Republic of Srpska, Banja Luka, Republic of Srpska, Bosnia and Herzegovina milan.latinovic@live.com

Public Key Infrastructure (PKI) is a platform that provides public networks users, such as Internet, secure transactions of dates and money. Prime goal of this paper is to define main terms of PKI systems and finding of existing analyzes that describe their planning and realization. The aim of this paper is to provide basic information to institutions that are thinking about progress with introduction of the above mentioned systems.

Key aspect of SKI system is **security** that is accomplished with usage of symmetric and asymmetric cryptographic algorithms. Cryptology is a term from Greek words *krypton* (hidden, secret) and *logos* (science) and is used discipline that deals with secure communications. In proceedings two disciplines of cryptology are analyzed: cryptography and cryptanalyzes.

By cryptography methods and algorithms for providing of information secrecy are studied, while **cryptanalysis** observes methods and algorithms for violation of the same.

The main function of cryptography in SKI systems are defined as follows: [1]

- data protection – information are available only to authorized users,
- authencity – possibility of checking and guarantee of identity of participants in communication,
- data integrity – possibility of detection of unauthorized data change, and
- Non-repudiation of transactions – prevention of possibility of denial of realization of certain activities of participants in communication (such as messages sending, transactions etc.)

Besides competence in cryptography methods and algorithms, introduction of PKI systems will imply and familiarizing with directives, standards and local lows from this area.

PKI SYSTEMS

A key aspect of PKI's security, which is achieved by encryption of data. Basic cryptographic algorithms may be grouped as follows:

- Symmetric algorithms and
- asymmetric algorithms.

A special place in the cryptographic systems take up functions for creating prints (Eng. Hash functions), which are closely related to the electronic signing of documents and processed in the next section.

Symmetric cryptography is the oldest form of cryptography. Basic symmetric cryptographic algorithm has defined and introduced in 1949. C. Shannon [2]. This method of cryptography implies knowledge of the algorithm which

performs encryption and encryption key that must be known only to the participants in the communication. So every two users in communication must have and use a common and unique private key. The working principle of a symmetric cryptographic system, is shown in Figure 2.1.

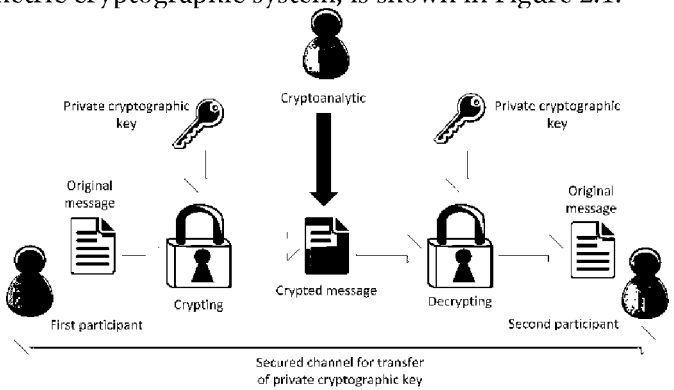

Figure 2.1. – *Principe for functioning of symmetric cryptograph system*

The main disadvantages of symmetric cryptography are:

- problems of distribution of keys – how to deliver the keys to the communicating parties, without compromising in the process of delivery, and
- a large number of keys required for communication between multiple users - namely the n participants in the communication, the n (n-1) / 2 keys.

Asymmetric cryptographic algorithms (Eng. Asymmetric Key Algorithms) are cryptographic algorithms where the encryption and decryption use different keys. Each participant in the communication has a cryptographic key pair, i.e., private and public key. The public key is available to all participants in the communication, while the private key is known only to the owner of the key.

Communication is established by using the pre-arranged transmission of the channel and encryption of messages exchanged is performed using previously exchanged public keys and private keys that are known only to owners, that is, the creators of individual messages. The working principle of asymmetric encryption system is shown in Figure 2.2. Today's PKI systems are based on a combination of symmetric and asymmetric cryptographic algorithms and hash functions.

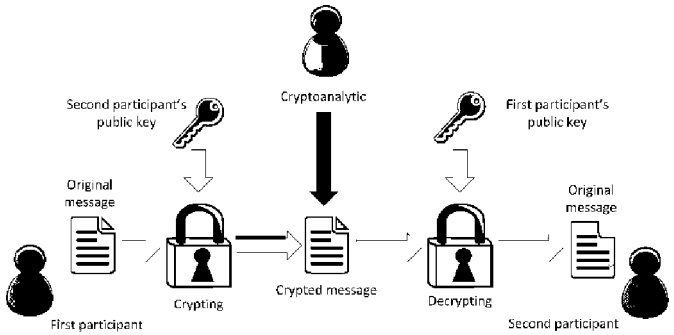

Figure 2.2 – *Principle of functioning of* asymmetric cryptographic system

There are two general problems with the PKI systems:

- the amount of data that need to be encrypted and
- time for calculating of asymmetric functions for encryption.

Hash functions are classified in cryptographic algorithms without a key. According to [3] the basic idea of the hash function is to create a print of the document that is encrypted. Basic characteristics of the print is that it is considerably smaller than the original document and clearly describes the document. Using these functions to the document, it is obtained the print that is easier, faster to encrypts, which in addition, prove the identity of the document and non-repudiation of documents.

According to [4], PKI systems are a combination of hardware and software products, policies and procedures related to allow users who do not know or do not have physical access to each other to communicate securely through a network of trust.

Confidence in PKI systems is based on digital certificates. In practice, the term digital identities (Digital ID) is also used. Digital certificates link user identity with their digital signature, and in practice the term electronic signature has also been used since

The basic components of a PKI system are:

- Certification policy (Eng. Certificate Policy - CP)
- Practical work rules (Eng. Certificate Practice Statement - CPS),
- Certification body (Eng. Certificate Authority - CA)
- registration Authority (Eng. Registration Authority - RA)
- systems for the distribution of certificates (Eng. Certificate Distribution Systems - CDS), and
- PKI applications.

CP sets out the basic policies of the certification body and other components of the PKI system. Basic policies includes the manner of publication of official documents on certification and their location, means of identification and authentication of users, writing the application for the issuance and withdrawal of digital certificates, electronic security and control of the protection profile certification, audit methods and legal issues.

CPS is a practical document that describes the operation of the certification body. In practice, the CPS represents a detailed elaboration of the basic policies of the certification body.

CA is the basis of trust and a major component of the PKI system, with the main tasks: generation of digital certificates, governing of certificate life cycle and providing mechanisms of withdrawal and re-activating of digital certificates.

RA provides an interface between the user and the CA, which accepts requests for the issuance of digital certificates, checks the validity of these certificates, but they do not approve them. RV forwards it to CA. Thus RA has a role of Preprocessor of CA, with a significant role of verifying of users' identity.

CDS in practice can be solved in two ways: direct transmission or distribution of certificates to customers through directory server. Definition how the distribution of certificates and their validity checking is out of the scope of this paper.

PKI applications include software solutions for: digital signing of documents, the security of the web server and email servers, Web transactions, virtual private network (Eng. Virtual Private Network - VPN), access control systems and similar.

ELECTRONIC SIGNATURE

Law on Electronic Signature of the Republic of Srpska defines an electronic signature as a set of data in electronic form which are attached to or logically associated with other data in electronic form which are used to identify the signer and the authenticity of the signed electronic document. Also, qualified electronic signature is defined as electronic signature that reliably guarantees the identity of the signer and that:

- is linked exclusively to the signatory,
- indisputably identify the signatory,
- created using means that the signatory can independently manage and that are exclusively under the control of the signatory, and
- is directly linked to the data to which it relates in such a way that unambiguously provides an insight to any amendment to the original data.

In practice, the electronic signature is the process by which a particular block of data or a portion of the block cryptographic is marked by Signatory secret parameter. As noted above, each participant in the PKI system gets its pair of keys: a public and a private key. The public key is available to all participants of the PKI, and the private key is known only to its owner. In case the private key becomes known to anyone beside its owner, all electronic signatures created by this private key are compromised.

The procedure of electronically signing of the document, shown on Figure 3.1. can be viewed through three phases:

The first phase alludes to implementation of function for creation of the print, such as message – digest algorithm – MD or secure hash standard – SHS.

In the second phase the acquired print is encrypted by secret key of the user, by usage of adequate asymmetric cryptographic algorithm, such as RSA.

In third phase the encrypted print is added at the end of original message and acquired data blocks are sent to recipient or recipients.

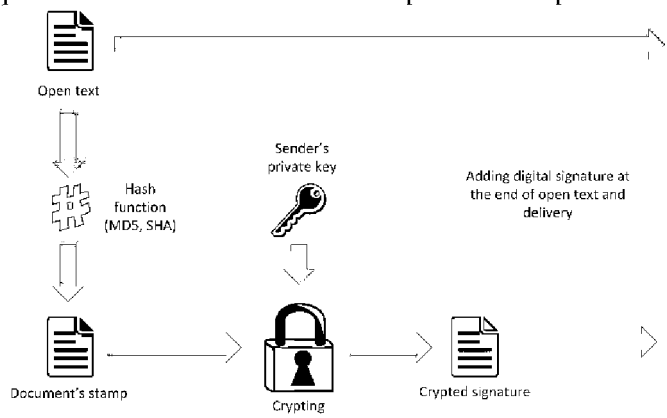

Figure 3.1. – *Creation of electronic signature*

The procedure of electronic signature checking, shown on Figure 3.2. can be seen in three phases:

The first phase means the reception of electronically signed document and separation of original message from the electronic signature.

The second phase is re-using of hash function onto original text. This function must be suitable to the original hash function that was used during making of electronic signature.

The third phase means comparison of the print that we got by hash function usage and the original print. If mentioned prints are identical, then the validity of electronic signature is proved. On the contrary, the document is

considered compromised, as well as private key of the sender, which is the document signer.

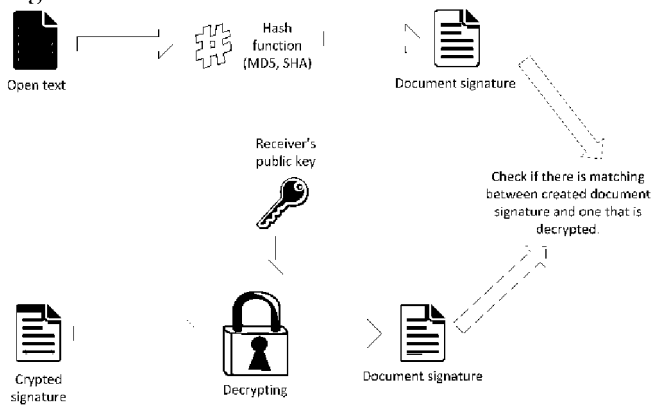

Figure 3.2. - *Checking of electronic signature*

There are many companies that offer ready-made solutions for PKI systems, simple for implementation inside some institution or business process. The security of these PKI systems depends on algorithms and longitudes of the keys used for scripting.

DIRECTIVES AND STANDARDS

Directive is a legal document of the European Union (EU) by which a certain result is demanded from the member states, without given guides how to reach the demand results. The Directive demands implementation, unlike the Regulative which is self-sustainable.

When we talk about SKI, basic directive of the EU are:

- Directive 1999/93/EC Of The European Parliament and Council, and
- Comity's Decision 2003/511/EC.

Directive 1999/93 EC has for the goal facilitating of electronic signature usage through creation of needed legal frames. [5]. Committees' decision 2003/511/EC is not obligatory, but presented as recommendation that states on the security demands of electronic signatures and products based on them[6]. The concrete list of standards is given and grouped according to annexes of this Decision.

The organization Internet Engineering Task Force (IETF) consists of numerous working groups that work on the development and promotion of IKT standards. All developed methods, observations, recommendations,

research and innovations are published in so called **Requests for Comments – RFCs).**

Basic RFC documents connected to PKI are:

- RFC3820 - X.509 PKI, profile of proxy certificate,
- RFC2560 - X.509 PKI, Online Certificate Status Protocol – OCSP),on--line protocol for certificate's status display
- RFC3647 - X.509 PKI, polices and usual practices of certification,
- RFC2511 - X.509, message format certificate demand,
- RFC2797 – certificate managing messages CMS,
- RFC3039 - X.509 PKI, qualified certificate profile,
- RFC3161 - X.509 , PKI, Time-Stamp Protocol, and
- RFC3281 – Attribute profile, used for authorization of certificate.

International Telecommunication Union – ITU

Has issued **ITU X.500**, recommendation for data base appearance intended for global usage as directory where every organization manages its own part of the directory. Such global data base is necessary for existence of global PKI system inside which there are no redundant dates. [7]

ITU X.509 is a recommendation for structure electronic certificates. It was published for the first time in 1988. As part of ITU X.500, after that version 2 followed in 1993. and version 3 was published in 1996. This version is still active.

X.500 was not accepted wider, but X.509 set its ground, and it is now basic for providing services of digital certificates.

Based on X.509, on Figure 4.1. structure of digital certificate is presented.

Form Version x.509.
Certificate serial number
Single-valued identity code
Algorithm used for digital signature (SHA1/RSA, MD5/RSA)
CA title that issued the certificate sertifikat
Period of certificate's validity
Certificate's owner, according to X.500
Dates on public key of the signature
Usage certificate conditions
Digital certificate signature with secret key of Certificate body

Figure 4.1. – *Structure of digital certificate*

LOCAL LOWS AND REGULATIONS

According to the Regulation of Republic of Srpska Government Low and Public services system low, on December 26th 2007, Republic of Srpska's Government made decision of creation Public Institution 'Agency for IT Society of Republic of Srpska' (AIDRS). By this Act Republic of Srpska got the institution with the duty of following of development of IT society and promotion of IKT usage, and under government of Ministry for science and Technology.

One of the main functions of AIDRS is creation of legislative necessary for introduction of PKI system in Republic of Srpska, after which, the concrete implementation of these systems is predicted.

In Republic of Srpska for PKI systems usage, following lows exist:

- Low on electronic document of RS,
- Low on electronic signature RS, and
- Low on electronic conduct in RS.

Previously mentioned Lows are amended with following subordinate legislations:

- Act on electronic certification holders,
- Regulations on certification body evidention,
- Regulations on electronic signature protection measures, the lowest amount obligatory security and usage of organizational and technical measurements certificate protection,
- Regulations on the content and the way of managing Certified Body Register for issuing of qualified electronic certificates, and
- Regulations on technical rules for securing the connection between evidention issued and withdrawn Certified Bodies in Republic of Srpska.

SECURITY OF ACTUAL CRIPTOGRAPH ALGORITHMS

As security of PKI systems completely leans on security of cryptograph algorithms used for scripting / descripting as part of PKI, it is extremely important to provide and use such cryptographic algorithms that provide high level of security. Up today tens of cryptographic algorithms have been created that are still in use in SKI systems and provide very good security and protection of high level.

There are several scientific-research groups in the world that deal with security estimation of algorithm, and they periodically give recommendations of key longitudes that should be secure for usage in the period of next five to eight years. One of such groups is ECRYPT II, that works under the demand of European Commission on Cryptographic algorithms and key

longitudes that are secure for usage. In The Annual Report for 2008-2009 [8] given on July 29th 2009. the group gave the recommendations on the keys longitudes.

For estimation of **minimal longitude of symmetric keys** rather clear principle is used for calculation of time needed for breaking through of key with the attack

With brute force or with guessing, with which success of braking through depends only on available process power. Calculation on key longitude is done according to available process power P and time needed for protection of the dates, for which is usually taken life span of the protected dates. Accordingly, for minimal key longitude is taken n-importance longitude, such that $2^n/P$ is sometime longer from the life span of the data (the time of data protection). Recommended key longitudes classified to the groups of attackers are given in Table 5.1

Attacker	Available		Min. Long.	Breaking through time
	budget	hardver		
„Hacker"	0 USD	PC(s)	53	222 days
	400 USD	FPGA	58	213 days
Small organization	10k USD	FPGA	64	278 days
Medium large organization	300k USD	FPGA/ASIC	68	256 days
Large organization	10M USD	FPGA/ASIC	78	68 days
State agency	300M USD	ASIC	84	64 days

Table 5.1. – *Recommended keys longitude in 2009.*

As for the evaluation of the minimum »safe » length of asymmetric keys, things are a little more complicated because unnecessarily large keys can significantly reduce performance, there is a significant and constantly growing number of attacks that were discovered in the past 30 years and that give results much faster and better of brute force attacks and the occurrence of special crypto-analytical hardware that is significantly more than the » naive » machine - browser (end. Search - Machines). Moreover, symmetric and asymmetric schemes (algorithms) are often used in combination - for example the asymmetric key is often used to protect a symmetric.

As greater length keys significantly affect the performance of encryption, it is important to assess the length of the keys are sufficient to provide any level of data security. Some key length well-equipped organization can break in a relatively short period of time (on the order of 60 to 90 days). Therefore, it is more than interesting to do a review of the length of symmetric keys by an estimated breakthrough time. This classification is given in [5] and is shown in Table 5.2, where * is the level of protection, and ** represents the minimum length of a symmetric key.

*	**	Level of protection	Comments
1.	32	Individual attacks in real time	Should not be used in the development of new systems
2.	64	Very short-term protection against small organizations	
3.	72	Short-term protection against medium-sized organizations, and medium--term protection against small organizations	
4.	80	Very short-term protection agency , long-term protection against small organizations	The lowest recommended level of protection for general purposes , which provides up to 4 years of protection
5.	96	The standard level of protection	The recommended level of protection for general purposes ; Provides data protection for up to about 10 year
6.	112	Mid-term protection	Provides data protection for up to about 20 years
7.	128	Long – term protection	A good level of protection and recommendations and to protect the most important data ; Provides data protection for up to about 30 years
8.	256	Long-term protection for the foreseeable future	Good protection of the quantum computer

Table 5.2. – *The recommended length of symmetric keys by levels of security, 2009.*

REFERENCES

1. D. Đorđević, „Digitalni potpis i digitalni sertifikat“ TELFOR, pp. 1, novembar 2007.
2. C.E.Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, 1949, pp. 656-715.
3. Bart Preneel, Analysis and Design of Cryptographic Hash Functions, 2003.
4. M. Marković "Infrastruktura sa javnim ključevima (PKI – Public Key Infrastructure)", pp. 9-11.
5. J. Dumortier , "The Europian Directive 1999/93/EC on a Community Framework for Electronic Signatures" , december 1999.
6. E. Liikanen , "COMMISSION DECISION 2003/511/EC" , july 2003.
7. I. Curry, „Version 3 X.509 Certificates, Entrust Techonologies", 1996.
8. Grupa autora European Network of Excellence in Cryptology II mreže, „ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009)“.