Yugoslav Journal of Operations Research
Vol 19 (2009), Number 1, 185-194
DOI:10.2298/YUJOR0901185P

REDUCING E-COMMERCE RISKS USING DIGITAL CERTIFICATES

Miloš PIŠČEVIĆ
Serbian Armed Forces, Belgrade
milos.piscevic@gmail.com

Dejan SIMIĆ
Faculty of Organizational Sciences, Belgrade
dejan.simic@fon.bg.ac.yu

Received: December 2007 / Accepted: May 2009

Abstract: E-commerce means buying and selling goods and services across the Internet. Secured communication in e-commerce, across unsecured medium, such as the Internet, represents one of the major components in a domain of providing necessary security-critical demands, so the flow of information could go in a secure way. The Internet, as a global computer network must provide five major security services: confidentiality, data integrity, authentication, availability, and non-repudiation of information. Without guaranteeing aforementioned security goals, risks may be very high in e-commerce systems. A possible way to reduce these risks is to use digital certificates. Digital certificates provide a means of proving identity in electronic transactions, and from the point of view of computer communication they are irreplacable, but nevertheless they provide a good mechanism for implementing the major part of this security goal, and therefore, their usage in e-commerce is the major topic of this paper.

Keywords: Cryptography, digital certificates, X.509, e-commerce.

1. INTRODUCTION

E-commerce represents a set of technologies and procedures which automates business transactions via electronic devices. Information is transferred via e-mail, EDI (Electronic Data Interchange) system or through a World Wide Web service – the Internet. In general, e-commerce stands for shopping and selling information, products

and services through a computer network and it is a support for any type of business transactions through digital infrastructure.

Modern computer networks are, almost entirely, based on Internet technologies and TCP/IP (*Transfer Control Protocol/Internet Protocol*) protocols. Automatized information systems, based on Internet technologies, have numerous weaknesses from the aspect of data security, which is caused by the computer network architecture of Internet/Intranet type:

- TCP/IP protocols are not projected to accomodate demands for information security
- Internet is a network with a package commutation in which an access to the information in the transfering process is relatively easy and the insertion of messages from an unknown source and content is possible

In order to solve these foregoing problems, as well as to support the Internet evolution, specialized software and hardware security systems are also developing. Nowadays, there are numerous manufacturers who produce, technologically speaking, high-grade quality products for a different level of security of modern computer networks. Public "de-facto" standard cryptographic algorithms are integrated in these products.

Cryptography is a technique which studies mathematical ways of generating messages, whose payload is known only to the granted users. According to this, with cryptography appliance, the realization of the following four major security services is made possible:

- confidentiality,
- authentication,
- data integrity, and
- non-repudiation.

Furthermore, a major service, namely **availability**, not acquired by the use of cryptography, has to be accomplished due to the information flow. It is concerned the fact that the qualitative information has to be available at any time, anywhere, even if the communication link is an unsecured media, such is the Internet.

While confidentiality is acquired through the usage of symmetrical cryptographic algorithms, the other services are employed with the usage of asymmetrical cryptographic algorithms. The modern solutions of security system are characterized by a multilevel architecture, with the usage of hardware security modules, HSM's. With the usage of HSM's, the most common thing to accomplish is the protection of security-critical data, such as cryptographic keys, user passwords and private security algorithms, the realization of cryptographic algorithms and other security functions independently from the other programs on a PC and the acceleration of cryptographic algorithms completion in relation to the systems based on the entirely software-based security methods.

2. PROBLEM DESCRIPTION

E-commerce reduces business costs and alleviates management even though there are potential risks when using this technology. For instance, electronic infrastructure is sensible to the different forms of attack. From the economic point of

view, the consequences of technological nature failures or abuse of this tecnology by end-users could besignificant, from losing an important information to reducing a business reputation and clients' confidence.

Because of the aforementioned problems, the consumers who use such services of e-commerce could experience direct or indirect financial losses.

Risks that follow e-commerce could be avoided with the use of adequate security measures. These measures could be the technological and the legal ones. The technological measures are concerned with authentication, confidentiality, data integrity and non-repudiation. What is necessary for putting these measures into practice is the use of cryptological technologies, e. g. the use of digital certificates.

As far as data security is concerned, the potential threats to an information system that holds e-commerce subsystem are:

- System infiltration – the possibility of an unauthorized person accessing a system and modifying files in order to detect confidential information and use the system resources in an illegitimate way.
- Authorization overload – when a person authorized to use a system uses it in an unauthorized way.
- Suplantation –after a successful infiltration into a system, an attacker usually leaves a program inside which will enable him to alleviate his/her future attacks. A class of suplanation is „the trojan horse".
- Eavesdropping – an attacker can access a confidential dataflow by eavesdropping easily inside a communication network.
- Data changing on a communication line – an attacker can change the information transferred through a communication line.
- Service denial – because of the occasional requests for complex tasks execution issued by the unauthorized system users, system services can become unavailable for the authorized users.
- Transaction negation – after a transation is completed, one side can negate that the transaction has actually happened.

3. PROPOSED SOLUTION

This paper is proposing the risk decrease in e-commerce systems with the usage of digital certificates. At the very beginning, it is necessary to make or buy an application for Certificate authority which will generate digital certificates. A generated digital certificate can be used in various ways. One of the most common usage is in S/MIME protocol, which enables the sending of secured e-mail messages, in the terms of digital signature and digital envelope. Nevertheless, this paper is mainly focused on the usage of digital certificates in e-commerce in e-payment process where the employed security concept utilizes asymmetric cryptographic algorithms and SSL protocol.

The solution to the system for generating digital certificates practically represents a segment of public key infrastructure. PKI facilitates the creation of the surroundings for the confident usage of e-business and it is usually based on the application of symmetrical and asymmetrical cryptographic systems. The foregoing infrastructure consists of more components, applications and documents which define a

way to realize the four major security services. System architecture of PKI is shown in Figure 1.

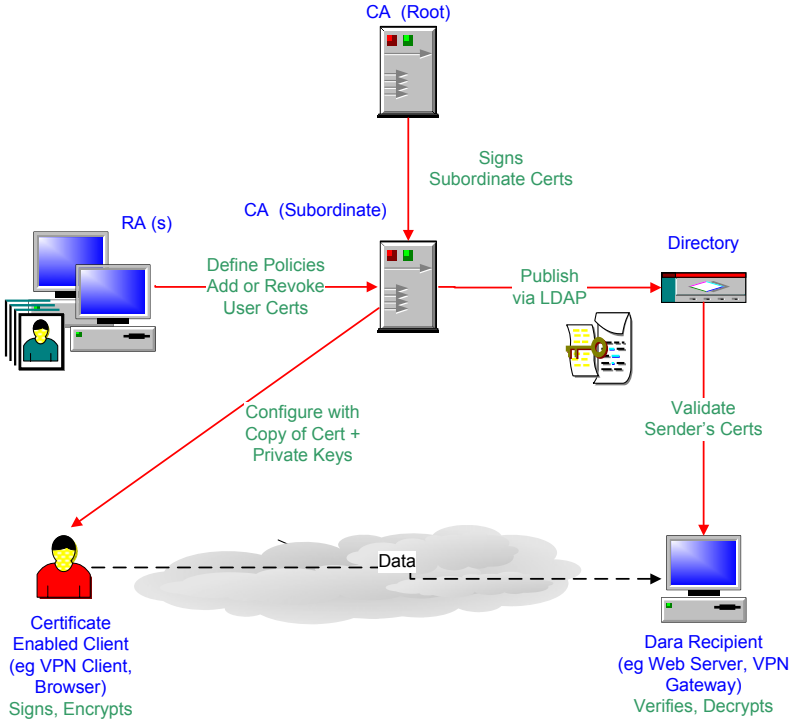

Figure 1. Public key infrastructure (PKI)

Namely, a certificate represents an unavoidable segment of business communication and e-commerce systems nowadays. The technology of digital certificates is extremely comprehensive. That is no surprise having in mind that the development of its foundation theoretically dates back from the 1970's and continues without stopping until today. The purpose of digital certificates is the maximum identification of a person or a system and the maximum data privacy. Many procedures around the globe are still developing, and they can be different in different countries.

Digital certificate is a data structure whose goal is to securely connect the public key on one side and the data regarding their carrier on the other side, ensuring the identity check by means of digital signing, for example. In modern security systems, the main carriers of digital identity are digital certificates.

There are two types of certificates, the self-signed and the qualified ones. Technically speaking, they are equal, but the self-signed certificate can be issued by everyone, i.e., we can do it by ourselves. They are mainly used internally, or the „legal force" is acquired by signing a special contract with the user (like in e-banking systems).

Far more important are the qualified digital certificates which, according to the Law on digital signatures and the inherent sub-law acts, can be issued only by a certificate authority that fulfills certain legal conditions and has a licence to work.

A qualified digital certificate with certain key pairs can be used for the creation of „a qualified digital signature“ of e-document, which is, in the terms of law, equivalent to the regular paper signed in the common way – with a pen and a stamp.

The internal data and structure standard of a digital signature is X.509, which has had three versions since 1988. The main improvement in version 2 is the introduction of unique identifiers of the issuer and the carrier, and in version 3, the introduction of so-called, “extensions”. Extensions are important because they essentially enable an entry of a wider range of data into a digital certificate.

The process of issuing a digital certificate begins in so-called Registration Authority. A request for a certificate issuing is delivered to the RA, which contains a personal data of a client. The RA’s job is to check these data and if they are correct, everything is set up for the preparation of a certificate request.

A client gets a card which is printed, but contains neither a digital certificate nor cryptographic keys. The user, with the attached software, generates a pair public/private keys on the card itself and runs a procedure of creating a request for issuing; the request is fulfilled with the necessary data and a complete digital certificate is almost made. The document prepared in such a way is sent to the Certificate Authority whose main task is to sign it digitally using its private key. This way a digital certificate is formed and sent back to the client who can use it by employing the specialized software and storing it on the card. The private key never leaves the card, which is one of the most important reasons why this system is considered reliable.

The Certificate Authority, or the CA, is an entity which signs the received demands for digital certificates digitally, generates the Certificate Revocation Lists, etc. The CA is necessary in the process of issuing a digital certificate because it represents a trustworthy institution.

4. IMPLEMENTATION OF PROPOSED SOLUTION

The programmed solution is carried out in Java programming language. Java Specification incorporates two relatively independent parts: Java programming language specification and Java Virtual Machine, JVM, specification [2]. Java programming language specification does not differ from the other object-oriented language specifications, while the JVM represents an innovation in relation to the other object-oriented languages of universal purpose. Java Virtual Machine specification represents a platform for the running of programs whose base is the programming model of imaginery – Java processor. Programs written in Java programming language are compiled for running on Java platform. In fact, an output of the compiling process represents an appropriate sequence of bytecode instructions – assembler directives of the Java processor. To run on an adequate computer platform, the existence of an appropriate interpreter is necessary, since it accomplishes the functionality of imaginery processor in the way of mapping an assembly of bytecode instructions into an assembly characterized for a target platform.

The consequence of this policy is the lower efficiency of Java programs, with the assured portability on all computer platforms for which the JVM is realized.In order to increase the efficiency of Java programs, JIT (*Just-In-Time*) compilers are used, since they can accelerate a program execution from 10 to 50 times [4] under certain

circumstances. The main idea of JIT technique usage is to compile Java bytecode instructions during the first call that the method consists of into a sequence of instructions directly running on a concrete platform (*native code*). Every next call of this method is directly mapped into sequence of instructions that are directly executed [4].

The introduction of the original portability concept on the level of source code has numerous consequences. This concept has become widely employed in the world of smart cards and mobile phone manufacturers thanks to the capabilities it spreads, making it possible to develop a software for a huge number of microcomputers produced by different manufacturers (with a Java support) identically and with the usage of the same programming language[3] [5], [6], [7]. This represents a great difference compared to the time when every manufacturer defined the assembler instructions typical for their own microcomputer families.

The main goal of the architecture design in the Java cryptographic subsystem has been to break the cryptographic behaviors apart from the methods of their algorithm implementation. It is rationalized in such away that different subjects are enabled to implement their own cryptographic algorithms and functions. The provider architecture has a goal to define the standard interface towards which a programmer uses its cryptographic functions, independent of the concrete algorithms or their implementation. In continuation, a few words are going to be told about the classes that represent the backbone of the cryptographic subsystem and the principles it is established upon.

Provider is a class from the **java.security** package which connects the algorithm names to the names of the classes which realize them. It is generated from the Properties class defined in Java and it represents an associative array whose key is the algorithm name, value accessed – the full name of a class which realizes the given algorithm.

Security is a class from the **java.security** package which contains a list of providers and methods typical for the lists used for adding and deleting elements, etc., and for which all the methods are static. In that way, having only one object of Security class is enabled. In terms of the algorithm implementation enabled by certain providers, it is necessary to register a given provider – to add it to the list of Security object [8] [9].

The application can be done with the usage of the Bouncy Castle provider (http://www.bouncycastle.org), but in such a way the platform independence would be constrained, because it would be necessary to possess those packages by the Bouncy Castle provider. The solution is strictly established in the Java Development Kit 1.6.

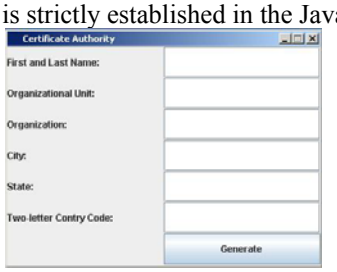

Figure 2. Application for generating a digital certificate

The application realized in Java programming language is shown in Figure 2. After the data input and the initiating of a button used for generating a digital certificate, the output is shown in Figure 3.

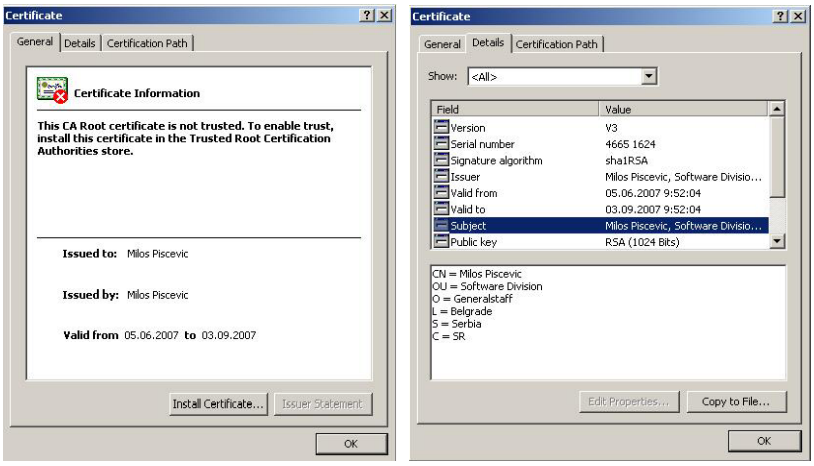

Figure 3. An example of a generated digital certificate

Asymmetrical cryptographic algorithms are based on the existence of key pairs: the public and the private ones. A private key is strictly kept secret which is known only to the owner of the key pairs, while his public key is available to all subjects of communication. A strong connection between a private key and his owner is achieved by digital certificates, on the basis of the digital signature and the technologies which enable the reliable functioning of a public key infrastructure. The structure of a digital certificate is shown in Figure 4 [10].

Figure 4. Digital certificate structure

Digital certificates practically represent the unique identification parameters of the subjects in communication. We can call them "digital personal id cards", because they are actually that – a digital personal id card in cyber space, a device that can enable two persons communicating via the Internet to prove their identity.

Elements that make the digital certificate structure are:

- A certificate format which represents a digital certificate indicator. One of the most commonly used digital certificate formats is the X.509 standard. The last version of this standard is version 3.

- Every certificate issued by a Certificate Authority has its unique serial number. A certificate is uniquely defined by the name of the Certificate Authority which issued it and with its serial number.
- The validity period of the certificate represents a time period in which the issued certificate is valid. In high security systems, digital certificates are issued for the period of six months or shorter, because of the crypto-analysis attack.
- A certificate owner is represented with a complex structure which contains the following personal data:
- The owner's name,
- The organization name in which he/she is employed,
- The name of the lower organizational part,
- The city name,
- The two-letter country code,
- The region within the state.
- The certificate is digitally signed by the Certificate Authority that issued it. The certificate integrity is guaranteed by this signature.
- For the purpose of checking a digital signature, one of the fields of digital certificate is the signature algorithm used for the digital signature creation [11].

The role of a digital certificate is to physically connect a subject ID with his private key. The creation and the digital signing of certificates is made by "the *trusted third party", TTP*. So if the receiving side successfully verifies a received digital certificate, it is then certain of the sender's authenticity – the owner of adequate private key.

5. ANALYSIS OF IMPLEMENTED SOLUTION

From the aspect of realization, the output of the system is a digital certificate. Nevertheless, a generated self-signed certificate has no extreme importance in e-commerce domain because of the non-signing process by the Certificate Authority, which guarantees a validity of such a certificate. The Certificate Authority can be observed as a guarantee for the subjects in communication in case of the security violation by one of the subjects in communication. If there is a need of using that generated digital certificate in a business communication, it is necesssary to define a request for issuing of a digital certificate, so that qualified digital certificate is gained.

A good side of this system is the platform independence which it possesses. This is above all due to the fact that the main programming language chosen is Java, produced by the Sun Microsystems, Inc. But on the other side, the major disadvantage is the solution performance and the open source policy. Firstly, it is well known that the C++ programming language has better performance than the Java programming language, and secondly, Java Obfuscator is necessary for the protection of an open source code, since there are many Java decompilers for Java's bytecode, and the system security is at stake.

6. DIRECTIONS OF FURTHER DEVELOPMENT

Directions of further development can be numerous, but limited by the possibility of usage and actual needs:

- The realization of own cryptographic provider (maybe a cryptographic subsystem,as well), with own implementations of symmetric and asymmetric cryptographic algorithms,
- The use of asymmetric cryptography standards – PKCS *(Public Key Cryptography Standard*) 1 – 15,
- The creation of certificate revocation lists, Registration Authorities with a certain interface for communication with the Central Certificate Authority
- The realization of the proposed security protocol on the level of application in the C++ programming language, for the purpose of the improvement of efficiency in relation to the existing realization,
- Other numerous usages, in accordance with the actual needs.

Foregoing possibilities of further development in terms of implementation with C++ programming language would certainly be necessary if the usage took place in a network authentication service domain, above all because of the performance.

7. CONCLUSION

Digital certificates, their concepts and usage in the area of e-commerce and Java Cryptographic Architecture are described in this paper as well as the authors' own ideas about generating a digital certificate. The significance of this paper is to point out the importance of digital certificates because they are a practical solution to many problems. The authors' idea was to examine the feasability of implementation of digital certificates in one single CA architecture for small organizations, and with small amount of assets. As one of the main precondition for safe and secured communication of subjects in a distributed environment, the usage of digital certificates is based on multilevel security architecture which exists nowadays as one of the possible defenses against potential attacks on computer systems. The main characteristics and concepts of Java programming and their consequences are also described.

The Internet evolution has made new terms for management and, as a consequence, the traditional working environment has changed. E-commerce has become an efficient method for regulating offers and requests on the market and, being supported by security systems, it represents the most economical environment for the presentation and placement of merchandise and services. Security system integration, in an integral system of e-commerce leads to the four basic aspects in security designing process: authentication, authorization, confidentiality and non-repudiation.

For the realization of reliable system for data confidentiality in an e-commerce system, what is needed is the use of combined security system on many levels, with software and hardware components, based on the usage of asymmetrical and symmetrical cryptographic systems, digital certificates issued by the Certificate Authority and the smart cards for generating of digital signature and safe-keeping of cryptographic keys. In laboratory conditions, the implementation of digital certificates, with the usage of Java technology, is successfully accomplished.

REFERENCES

[1] Behrouz,A., and Forouzan: *Data Communications and Networking*, http://www.mhhe.com/forouzan, The McGraw-Hill, 2004.
[2] Milosavljević, B., *Praktikum za kurs Java i Internet programiranje*, Military Academy, Belgrade, August 2001.
[3] Group Oriented Digital Certificate Architecture, http://www.ieee.com, 2007.
[4] Java Card 2.1.1 Specifications, http://java.sun.com
[5] Java Card 2.1.1 Runtime Environment (JCRE) Specification, http://java.sun.com
[6] Java Card 2.1.1 Virtual Machine Specification, http://java.sun.com
[7] Java™ PKCS 11 Reference Guide, http://java.sun.com/products/jdk/1.5/guide/security/p11guide.html, 2004.
[8] Knudsen, J., *Java Cryptography*, O'Reilly, 1998.
[9] Java™ Cryptography Architecture API Specification & Reference, http://java.sun.com/products/jdk/1.2/docs/guide/security/CryptoSpec.html
[10] Pistoia, M., Reller, D. F., Gupta, D., Nagnur, M., and Ramani, A. K.,: *Java 2 Network Security*, International Technical Support Organization, http://www.redbooks.ibm.com,1999.
[11] Marković, M.,: *Tehnike zaštite podataka i kriptografski protokoli u savremenim računarskim mrežama*, 2004.