World of Computer Science and Information Technology Journal(WCSIT)
ISSN: 2221-0741
Vol. 1, No. 6, 264-268, 2011

Interoperability of Digital Signatures in Public Administration

Nicuşor Vatră
Doctoral School Department
The Bucharest Academy of Economic Studies
Bucharest, Romania
nicusor.vatra@yahoo.com

Abstract— Interoperability is becoming one of the technical terms used in the IT industry and this is due to the development of the Internet and the growing need to make different applications communicate to each other. Interoperability seen as critical in public key infrastructure (PKI) implementations, because are used to assess the ability of two PKI applications to interact, providing great flexibility in carrying out secure transactions between two or more organizations using different PKI technologies. In this paper, we present some public key infrastructure interoperability problems, and we identify an infrastructure for interoperability of digital signatures in public administration.

Keywords- digital signature; encryption; public key infrastructure; interoperability.

I. INTRODUCTION

One of the major characteristics of any electronic transactions performed on the Internet is trust. On the Internet, where is no straight contact among parties and millions of users exchange information daily is necessary to take security measures to validate our collaborators, customers and suppliers prior to the exchange information's, goods and services or make payments.

Public Key Infrastructure (PKI) provides the needed trust by means of Trusted Third Parties (TTPs) identified as Certification Authorities (CAs) [1]. These digitally sign data structures named Public Key Certificates (PKCs), confirming that a specific public key belong to a certain user. Therefore, certificates and their keys give the connecting information about their organization partners. The recipient of a certificate has to approve its signature and validity before trusting the certificate's content. If the same CA issues the certificates of the communicating parties, one can easily confirm the signature of other certificates using the public key of this CA., even so to confirm the signature of a certificate issued by another CA is necessary a certain trust relationship between the PKI authorities.

There are different paths to establish a trust link named "Trust Models." These permits to a user to create chains of certificates from its trusted CA to other users recognized as Certification paths.

II. DIGITAL SIGNATURE

Digital signature or digital signature scheme is a mathematical scheme used to prove the authenticity of a message or electronic document. A valid signature gives the recipient confidence that digital signature applied to the document was made by signatory and that it wasn't changed during shipment. Asymmetric encryption and digital signatures are used for sending secure messages through unsafe channels. Use of digital signatures and security gives the recipient confidence that the message was sent by the signatory.

One of the applications of public key cryptography is digital signature. Digital signature needs to meet the following general requirements [1]:

- To be authentic, that is executed by the document author;
- To be unskilled, is to prove that the document was produced by the alleged signatory;
- To be non-reusable, that cannot be moved by a malicious person to another document;
- To be unalterable, once the document signed, it cannot be changed;
- Be non-repudiable, that the signatory cannot later deny its authenticity.

Because the act of digitally signing of a document needs comply with existing legal rules as in the case of classical

signature, digital signature must have the following four attributes:

- To authenticate the signatory. A signature must indicate the person who signed a document, message or record and make impossible to reproduce by another person without authorization from the former;
- To authenticate the document. A signature should identify the document that is, making it impossible to counterfeit or alter his or her signature, without being able to see this;
- To be an affirmative act. Determines that a transaction was made legal;
- Efficiency: the optimal signature creation and verification processes provides maximum safety to both authenticate the signing and the document, with low resource consumption.

III. PUBLIC KEY INFRASTRUCTURE

Public key infrastructures (PKI) have become the starting point for modern security mechanisms on the Internet, PKI closely linked to the asymmetric key encryption, digital signatures and encryption services, but to enable these services are used digital certificates. PKI facilitates storage and exchanges electronic data in a secure way, safety ensured by using public key cryptography, and the types of security services offered [3]:

- *Confidentiality* - maintaining the private nature of the message, performed using encryption and the public key from a certificate to establish an encrypted communication channel is the result that only the recipient specified in the certificate (which is the owner of private key) will be capable to decrypt the message encrypted.
- *Integrity* - proof that the message has not been altered is obtained with the help of digital signature, and by verifying the signature successfully, that message has not been changed after signing. Authenticity - verifying the identity of an individual or an application which transmits the message is done using a digital signature.
- *Non-repudiation* - providing security as the certainty that the message cannot deny it later passed.

The services listed above are part of secure communications and these are an essential security requirement and dates from ancient times. In practical terms, this often means encrypting messages are transmitted in the Internet by email, file transfer; secure electronic transactions [4].

Public key infrastructure or PKI deal with key management encryption-decryption for different user groups to ensure confidentiality of information, more and check their integrity using digital signatures and non-repudiation, we could say that PKI is based on public key cryptography, digital signature and digital certificates [2].

IV. PKI INTEROPERABILITY PROBLEMS

Public Key Infrastructure (PKI's) are central parts of the security architecture within an organization, such an infrastructure provides an important starting point for security management and to develop new standards and specific applications to ensure security. Most standard protocols for e-mail security, Web access, VPNs use public key certificates and thus require some form of a PKI.

PKI is a system used to secure electronic communications and to create trust between entities in closed or open information environments. Trust between users is achieved through the exchange of certificates and authentication. However small, medium and large organizations are inclined to use PKI. There are numerous operational problems of PKI, which collectively known as interoperability issues. Interoperability between different implementations of PKI security infrastructure forms the basis of large-scale PKI environments [5]. Figure 1 presents the main PKI interoperability problems encountered in practice.

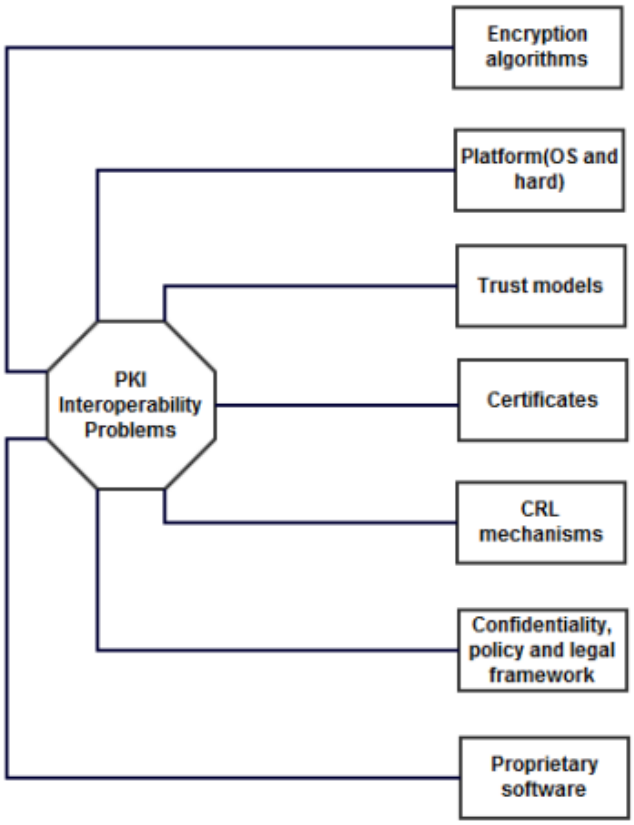

Figure 1: PKI interoperability problems

V. RO-PKI SOLUTION

Hire is described PKI solution and protocols used to interact with various entities that are part of this solution, is based on PKI. PKI components at conceptual level are

certification authorities (CA), registration authorities (RA) and end entities.

The architecture of a PKI consists of operational and security policies, security services and interoperability protocols that support the use of public key encryption and certificates management. There are three basic types of architectures, according to the number of existing certificate authorities [6]. In a PKI, RA usually processes the CA issued digital certificates and applications. Responsibility of the RA is to examine individual applications. RA is the component that checks the user ID, that request the issuance of one or more electronic certificates based on a policy of issuing digital certificates. Inform the CA that is closer, about the applicant level of confidence, and after checking the level of confidence that the certificate issue and are responsible for managing the entire lifecycle of digital certificates assigned to users. The CA also has the task of establishing trust with other CA sites by cross-certification. The term end entity refers to end users or devices that interact with different components taking advantage of using PKI schemes offered.

The solution is developed in a secure manner to assist electronic interaction at the central government institutional and local, but also for companies that interact with certain state institutions.

The goal is to develop a national wide PKI infrastructure for public administration. The main goal is to authenticate civil servants, to achieve exchange of public documents or classified secret service in a secure manner, and to promote interoperable PKI solutions easy to deploy and use.

Why use such a solution? The answer to this question is that can provide secure services anywhere.

The main challenges we solve with such implementation is a strong authentication, preventing theft of information and reduce the volume of printed documents. The main services that the application is made that allows authentication of users who have a valid digital certificate and are entitled to access such services, uses strong encryption, an audit log of when users access computer resources. Users can access the same certificate (or cryptographic device-token) a variety of authentication systems and computer applications in its own file encryption, a hard drive's authentication, remote access certain websites[7].

PKI's primary objective of national (RO-PKI) is to create a secure electronic environment that facilitates the exchange of information between central and local government. The main actors involved in this process are public institutions (central and local government), citizens, private sector participants such as providers of qualified certificates and other public organizations by the partnerships.

In a general approach the goals that we have in mind for RO-PKI solution are:

- A new goal is to provide logical, procedural and operational activities necessary support of public institutions using tools in the virtual environment;
- Another purpose of RO-PKI solution is to create the National Bridge Certification Authority RO- BCA;
- The last objective is to provide management services of public/private key and associated digital certificates, required to implement security solutions such authentication, authorization, confidentiality, integrity and non-repudiation.

RO-PKI infrastructure is developed on open standards and is interoperable with similar infrastructure. The main characteristics which give an added value then other infrastructure are:

- Is in accordance with national and European law;
- Based on open standards, hence eliminating interoperability issues;
- Provides support for applications signature, encryption and decryption for the information;
- Can be implemented with most commercial products on the market or developed on request by specialized companies;

A. Construction Stages

RO-PKI solution consists of several independent public key infrastructures such as those of ministries and a bridge type CA called RO-BCA, which will work with different classes of digital certificates, the objective being the protection of information transmitted in Intranet or Internet.

In process of designing a certification authority, we have identified five essential steps that need to be taken into account:

1) Economic stage.

Preparing a business plan and feasibility study for implementation of public key infrastructure, primary analysis and cost estimates.

2) Security stage.

Development of security policies is made to define measures and procedures to ensure IT security. The implementation of information protection system installation and customization of controls are selected. As an evolving information system, information protection system must be modernized in order to counter new threats.

3) Technological stage.

A PKI is a sophisticated, modular infrastructure. When designing an infrastructure should be an analysis of available products on the market, which would result from selecting an optimal solution to be installed, customized and managed properly.

4) Legal stage.

Legal issues involving the organization and operation of a PKI infrastructure. Since the digital signature is a tool for simplifying the authenticity and identification of documenst

when are electronically transferred via the communication channels. Basic functions involves CA's signature, their suspension, renewal, revocation and administration of registered certificates, the following requirements must be developed:

- Regulatory procedures that describe the types of documents that could circulate electronically;
- Methods and facilities for delivery of these documents;
- Rules of procedure for authenticating the sender of the document;
- Resolve methods for conflict situations, etc.

As a rule, we think that the team should be composed only in development of technical specialists; however, the establishment of procedural rules and related documents is a trivial task that should be deal by professional lawyers.

5) Stage of organization.

To ensure effective operation and security of critical components of the PKI, such as certification authorities, registration, must be produced multiple guidelines, regulations and other documents of organization. In practice this is hampered by the incompleteness of the existing legal framework. In addition, technology should reduce the electronic workflow and implementation is growing a lot.

B. Guidelines and regulations

Below we have identified a list of guidelines and regulations that must be developed, agreed and adopted within the organization that whants to implement PKI:

- Components (CA, RA, deposit certificates, end users);
- PKI functions;
- Areas of responsibility;
- Administration of deposit certificates;
- Procedures for resolving conflicts;
- Audit procedures;
- Security procedures;
- Rules of procedure for certified operations;
- Rules of procedure for accepting and processing license applications;
- Order to control physical access to hardware;
- Procedures for protection of keys.

RO-BCA is an authority created in order to ensure interoperability between existing PKI sites by establishing relations between the necessary cross-certification policies and managing shared specialized information stored on public directory servers.

RO-BCA allows a secure and authentic communication between businesses and public authorities. Public key infrastructure within individual organizations are interconnected through it, and certificates have been issued can be used beyond the barrier the local environment within the organization, so-called islands of identity. Thus, different business processes (like secure email, secure logon, secure eID, etc.) can be used beyond the guaranteed individual organizations.

RO-BCA acts as a single point of connection between central organizations and offers extensive services for the integration of new participants and functioning RO-BCA. Thus individual organizations no longer need to establish trust relationships between them, but each will have to establish relationships only single point of contact with national RO-BCA. Is sufficient to ensure that the electronic business processes with all other participants. This service allows establishing new business relations safety and security, reducing costs and implementation time and improve their business processes from which all participants benefit.

Admission to RO-BCA is made after obtaining an approval from the accredited authority, this first phase is simple and easy to do in order to achieve a high acceptance and gaining the advantages of using this technology. Following accreditation, commission takes the decision to accept or not connecting to the RO-BCA.

Figure 2 is shown the proposed architecture for the national RO-PKI. It consists of RO-BCA and other existing public key infrastructure within the public administration in Romania, which can connect to other private infrastructure. For example, we will use a certification authority for citizens and that of a commercial supplier.

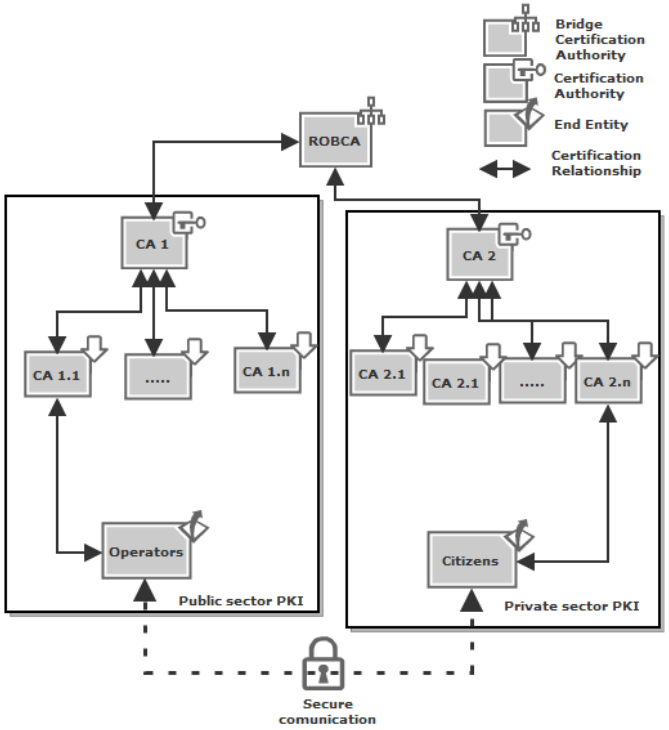

Figure 2: RO-PKI solutions

VI. CONCLUSIONS

The central element of an information system when using digital signatures is the certification authority involved in maintaining secure workflow. When building a PKI typically small and medium-sized organizations face two basic problems. The first one is because it is not profitable for a company to develop a PKI, especially where a company is not having an IT department and require high costs for hiring and training additional staff. A second problem is that if it is not accredited certification authority digital signatures within the organization will be recognized not only in its outside will not be considered valid by others.

Due to the rapid evolution of IT standards for building and protecting conventional exchange of electronic information systems in small and medium organizations prove to be in time inadequate. Username / password mechanism that are normally used when working with corporate information is an inadequate control even for electronic transactions within the organization, which are often subject to legal proceedings. Digital signature and encryption algorithms integrated in a PKI allow the construction of reliable information systems to ensure information security.

REFERENCES

[1] The European Parliament - 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 L 013 , 2000 .

[2] Thomas Jepsen - Distributed storage networks: architecture, protocols and management, John Wiley and Sons, 2003, ISBN 0470850205

[3] Carlisle Adams, Steve Lloyd - Understanding PKI: Concepts, Standards and Deployment Considerations, Addison-Wesley, 2003, ISBN: 0672323915.

[4] John Vacca - Public Key Infrastructure: Building Trusted Applications and Web Services, Auerbach Publications, 2004, ISBN 0849308224 .

[5] Nicușor VATRĂ - Public key infrastructure overview, Scientific Studies and Research. Series Mathematics And Informatic, International Conference on Mathematics and Informatics, Bacău, România, Vol. 19, No. 2, 2009, ISSN 2067 – 3566.

[6] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque - Public key infrastructure: implementation and design, John Wiley & Sons, 2002, ISBN 0764548794 .

[7] Nicușor VATRĂ - Public Key Infrastructure for Public Administration în Romania, IEEE Romanian Section Romanian Academy of Tehnical Sciences, The 8th Communications International Conference - COMM 2010, Proceedings Vol. 2, 2010, pg. 481 – 484, IEEE Xplore INSPEC ,ISBN: 978-1-4244-6361-9 .