"Vasile Alecsandri" University of Bacău
Faculty of Sciences
Scientific Studies and Research
Series Mathematics and Informatics
Vol. 19 (2009), No. 2, 471 - 478

PUBLIC KEY INFRASTRUCTURE OVERVIEW

NICUŞOR VATRĂ

Abstract. Public key infrastructures have become the starting point for modern security mechanisms on the Internet, PKI is closely linked to the asymmetric key encryption, digital signatures, digital certificate and encryption services. The purpose of this paper is to briefly describe the general and essential concepts of the PKI to persons interested in security and secure commerce but with a low knowledge level about the Internet security. That's why this study begins by introducing some basic security concepts, which are needed to understand the PKI topics. This document intends to be a good starting point for those interested in the PKI concepts, without analyzing particular implementations.

1. INTRODUCTION

The way people do business today is changing, the information is no longer circulated in the traditional way, at this time on e-mails circulate sensitive information such as contracts, classified information, financial information. Securing email, Web access, e-commerce, a VPN sites, and extranets need a strong security to provide confidentiality, authenticity, access control and data integrity. Nowadays, electronic information systems are complex as are the business processes that serve them, and one of the most important questions that should put us in any business transaction is electronic identity that makes the transaction. Using the scale of the Internet in electronic business, the need for confidentiality (C), integrity (I) and authenticity (A) of all those involved in these processes is vital, but to ensure these needs required the use of tools such as encryption or digital signatures, a very important tool in the continues fight for maintaining the CIA triad.

Keywords and phrases: PKI, security services, public key cryptography, digital signature, digital certificate Introduction
(2000) Mathematics Subject Classification: 68P25

Day by day, the Internet becomes an important means of communication and execution of electronic transactions, but as the volume of electronic business grows, and the growth is exponential appear the need for security of these transactions and to do that we have to create a security infrastructure such an infrastructure is public key infrastructure, it can speed up and simplify delivery of products and services through electronic approximation of the processes that have until recently been based on paper. This electronic solutions depend on the integrity and authenticity of data, both can be achieved by creating a link between a unique digital signature to an end user and ensuring that the signature cannot be spoofed.

Individual may then digitally sign data and the recipient can verify who sent data, and if they have been modified without the one he sent to know.

2. PUBLIC KEY INFRASTRUCTURE

Public key infrastructures have become the starting point for modern security mechanisms on the Internet, PKI is 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 is ensured by using public key cryptography, and the types of security services offered are:

- Confidentiality - maintaining the private nature of the message is performed using the encryption and use 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 able 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 altered after signing.
- Authenticity - verifying the identity of an individual or an application which transmits the message is done using a digital signature.
- Non-repudiation - property 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. 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.

3. PUBLIC KEY CRYPTOGRAPHY

The simple definition of cryptography is in equation (1), but the term cryptography comes from the words of Greek origin κρσπτός kryptÛs (hidden) and γράφειν gr·fein (to write), it represents a branch of mathematics, which deals with information security as well as authentication and restricting access to a computer system, and to early 70s was known only one type of cryptography that symmetrical. Asymmetrical cryptography or public key cryptography was invented in 1970 by James H. Ellis, Clifford cocks and Malcolm J. Williamson, who worked at the Government Communications Headquarters but was preserved as a military secret because GCHQ is a British intelligence agency. At five years after that Whitfield Diffie and Martin Hellman known researchers at Stanford University in California published in the journal IEEE Transactions on Information Theory an article entitled "New directions in cryptography", in this article have introduced a new method of key distribution exchange “Diffie-Hellman key exchange” with this method the authors have laid the foundations for asymmetric cryptography with public key.

It was developed to address two key issues namely, key distribution, namely how to have secure communication to communicate with a KD (center of distribution of keys) and digital signature to help you check that a message arrived unaltered from the one who sent it. It is asymmetrical because those who created the message or verify signatures cannot decrypt messages or create signatures.

Cryptography = Encryption + Decryption. (1)

Asymmetrical cryptography uses a single secret key and public key cryptography or asymmetrical uses two keys, a public key that can be known anyone and can be used to encrypt messages and verify signatures and the private key is known by the message recipient and can be used to decrypt and create signatures. Because is impossible other key deduction from another, one of the keys is made public, is set at anyone wants to send a coded message. Only the recipient, who holds the second key, private key can decode the message and use. Technical public keys can be used for email authentication feature, which increased its popularity.

The most important contribution of public key cryptography is that two or more persons can exchange messages safely without they have implemented comprehensive security solutions. The need to exchange private keys through secure channels as in the case of symmetric cryptography is removed, there is only exchanging public keys, private keys are not transmitted or shared. Among the most important cryptosystems public key is counting Egmal invented by Taher Egmal, RSA after its inventors Ron Rivest, Adi Shamir, Leonard Adleman, Diffie-Hellman and DSA, the Digital Signature Algorithm invented by David Kravitz.

A. Digital signature

One of the applications of public key cryptography is the digital signature, digital signature because it allows us to verify that a given private key to sign a message, and after checking to confirm the integrity and non-repudiation that message. The document they sign by creating a digital fingerprint of the electronic document is named (hash) and then encrypted hash with the private key of the author, then the person who sent the document and is the recipient decrypting hash with author public key, and it compares the current hash of the document, because at that time, the original hash was created with the private key, and if the two matches we guarantee that the author has created and signed the document, and that it is authentic. Digital signatures depend on two fundamental assumptions: It first is that private key is secure and that only the key holder has access to it, and the second is that the only way to make a digital signature is using the private key.

To obtain a digital signature are required eight steps:

- It creates a hash from message;
- It creates a digital fingerprint encrypted using the recipient's public key and obtain a digital signature;
- The clear message is combined with the digital signature;
- And the result message is sent;
- At reception, the message is separate from the digital signature;
- The message is decrypted using private key of the recipient;
- The message is hashed temporary in a digital fingerprint;
- It is used to validate received fingerprints, and it is checked if the message is authentic meaning was not altered during transfer.

B. Digital certificates

Digital Certificates are electronic files used in the identification of unique people and resources located in different networks such as Intranet, the Internet. At the conceptual level, we can say that a digital certificate is equivalent to ID or passport, as they are about the same functions and help in establishing identity. In short they show the association between public key of a person and that person, they are issued by a trusted authority called Certification Authority, the role of this authority is to issue a valid certificate after verifying the identity of the holder. A digital certificate generally includes a variety of information necessary for the CA that issued an owner, this information may include: an owner name, email address, public key, name of the certification authority issuing, identification number and a period of validity, and in creating the certificate information is digitally signed by the issuing Certification Authority.

Protecting private key is closely related to digital certificates, known as public key certificates. Implementation of a PKI depends on digital certificates, these certificates use digital signatures to make the connection between the user identity associated with public keys.

4. PKI COMPONENTS AND FUNCTIONS

PKI consists of a combination of hardware and software, policies and procedures that ensure the security necessary so that two users who do not know or are in various points around the globe can communicate securely. We saw that the PKI's digital certificates are a kind of electronic passport that maps a user digital signature to its public key and public key cryptography, but basically consists of a PKI will find in the following. A public key infrastructure involves collaborative processes among several entities: the certification authority CA, the registration authority RA, a deposit certificate, server recovery keys, and the end user.

In a PKI, the CA issue, manage and revoke certificates for one or more end users, and is responsible for their authenticity. As end users, CA is offering public key in the form of a signed digital certificate. As sites are divided into two categories: public and private, the public Internet operates providing certification of public and private is found inside organizations and in closed networks.

A registration authority (RA) is basically the interface between the user and the CA, check if user is authentic identity and send the request to release the certificate to the CA, an RA has the following functions:

- Check the information and accept the registration of new users;
- Generate keys on behalf of end users;
- It accepts and authorizes backup requests and recovery of keys;
- It accepts and authorizes requests for revoking certificates;
- After a certificate is generated must be saved.

After a certificate is generated it must be saved to be used later, and users no longer need to store certificates on the local machine, using CA's often a deposit certificate or a central store location. X500 deposits are very popular that behaves as deposit certificates and provides administrators a central location for entering personal information. Customers can deposit entries and assign attributes using access protocol called the Lightweight Directory Access Protocol (LDAP) certificate of deposit offers one point for managing and distributing certificates.

Even if we have a little or larger PKI, it will happen something that is inevitable some people will lose their private key, and loss may result because of a malfunction or a forgotten password. When this happens the CA must revoke the certificate with corresponding public key, then the new keys are generated and a new certificate automatically.

The main feature of the PKI is to ensure confidence in the exchange of information developed through the Internet or other electronic means, but the management protocols to assist the online exchange of information between users and management within a PKI, and functions that support them are:

- Registration: is a process in which the user wishes to obtain a certificate from the CA will present its attributes, either directly or through an RA, they are checked and then the certificate is issued.
- Initialization: Initial registration is followed by initialization, it involves the combination of user confidence.
- Certification: the process by which CA issue the certificate containing the public key of the user and then lodge in a public warehouse.
- Key Recovery: the keys can be used for creating and verifying digital signatures and for encryption or decryption, they can be recovered if the user loses the key, this CA-back or recovery system, and it is possible they must be submitted in a secured deposit.

- Key Updating: all key pairs and their associated certificates must be updated at regular intervals, because the certificates are issued for a certain period of time.
- Cross-certification: allow users within an administrative domain to use certificates generated by a CA in another operational area.
- Revocation: it appears at the expiration of the period of validity that may occur in the following cases: the change user name, the user is removed, private key is compromised. In the X.509 standard, to revoke a certificate using Certificates Revocation List (CRL).

5. CONCLUSION

As the part of Internet security has increased to contain gate-keeping roles as well as network facilitation, protecting information assets has come to be more costly and complex. The substructure for providing application and network security in this active environment is PKI. Since a successful PKI needs up to date technology, sophisticated certificate practices, and highly-trained employees, in-house deployment of PKI services requires important investments of time and money.

As a conclusion we can say that PKI is a security architecture that has been inserted to provide an increased level of confidence in the exchange of information in an increasingly less reliable as the Internet.

References

[1] C. Adams, S. Lloyd, **Understanding PKI: Concepts, Standards and Deployment Considerations**, Addison-Wesley Professional, 2 edition, 2002

[2] S. Burnett, S. Pine, **RSA Security's Official Guide to. Cryptography**, Osborne/McGraw-Hill, 2001

[3] R. Housley and T. Polk, **Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure**, Wiley, 2001

[4] B. Hammond, **Digital Signatures**, Osborne/McGraw-Hill, 2002

[5] V. Oorschot, Menezes, **Handbook of Applied Cryptography**, John Wiley & Sons, 2000

[6] V. Patriciu, M. Pietroşanu, I. Bica, J. Priescu, **Semnături electronice şi securitate informatică**, All, 2006

Faculty of Economic Cybernetics, Statistics and Informatics
The Bucharest Academy of Economic Studies,
Piata Romana 6, Bucharest, Romania,
nicusor.vatra@yahoo.com