Public Key Infrastructure (PKI) Implementation at ETF Sarajevo

Saša Mrdović
Faculty of Electrical Engineering
University of Sarajevo
Bosnia and Herzegovina
Email: sasa.mrdovic@etf.unsa.ba

Abstract

Building of public key infrastructure (PKI) at an educational institution is considered. PKI resolves many of the problems in the area of secure computer communications but is expensive and complex to implement. A paper suggests an approach to creating PKI that is feasible. Specific needs, environment and administration of a school at university are used to create custom made PKI. Given approach lowers the cost and level of complexity of building PKI and brings them within reach of an academic institution. Legal consequences of PKI implementation are examined.

***Key words**: Cryptography, Public key cryptography, PKI, Digital signature, Certificate Authority*

1. INTRODUCTION

The goal of this paper is to show that PKI could be implemented at Faculty of Electrical Engineering, University of Sarajevo, or any similar faculty for that matter. It has been said many times that PKI is hard. It is undeniably true, but there are some things that could be done about that. If one builds PKI from scratch for a big multinational corporation with a number of locations worldwide and a number of applications that need to be supported, it has to be tedious task. On the other hand, if we limit the scope of PKI, use existing infrastructure and administration wherever applicable, PKI could be implemented with resources available to a faculty in Bosnia. By limiting the scope of PKI, I do not suggest partial solution, but going back to basic ideas PKI was created for. There also must be clearly defined lower bound for the implementation. The solution must support all relevant standards and be scalable for future extensions. It should comply with applicable requirements set forth in Central bank's decision on minimal requirements for becoming CA [1].

I shall define our needs and explain how PKI satisfies them. I shall name main obstacles to wider PKI adoption. In a chapter on suggested approach, I shall explain core PKI components and procedures and suggest how each of them should be implemented at ETF. At the end, I shall present legal aspects of PKI implementation at ETF.

2. OBJECTIVES AND REQUIREMENTS

2.1. Objectives

Let us first define what we want to do. Only if we have a clear understanding of our goals we can start creating a solution. We would like people at our school to be able to use their computers to communicate in a secure fashion. Some of the services that users expressed their immediate need for and that should be implemented first are:

- The professors need to be able to publish official signed exam results on our intranet or the Internet
- The students would like to be able apply for exams online
- The dean and management need to be able to publish signed official school documents on our intranet
- Administration needs secure access to all official documents, exam results and students files and also means to publish the documents that need to be published
- All users of the system need secure access to all the documents they are entitled to see

This is not meant to be a complete list of needed or possible services, but just a sample of the results expected from this project.

2.2. Security services

Now, when we know what we want to achieve, next question is how. If we look again at the above list of requirements, we can define basic tasks the system needs to do.

Last requirement talks about secure access to predefined set of data. This is achieved through *authentication* and *authorization*. Users need to present to system something they know or they have or both that proves that they are who they claim they are. Then the system needs to check if they are authorized to access the data they requested. Students should not have access to documents intended for employees only, but also must not be denied access to their grades.

Users also need to be sure that the data they get was not altered in any way either at its source or on the way from the source to the user. Students must be sure that exam results they are looking at are the ones the professor entered. This is especially important in case that the data is being accessed through insecure channel, like the Internet is. System needs to guaranty *data integrity*. In addition to being sure that data has not been tampered with user also needs assurance that nobody eavesdropped on data while in transfer. This means that only intended recipients can see the data. System needs to guaranty *data confidentiality*.

With everything above achieved, the source of data, a user who created it, should not be able to deny doing so. The student that applied for an exam cannot claim that it was not he but somebody else. This is called *non-repudiation*.

Each of the above mentioned system properties, *authentication and authorization, data integrity, data confidentiality and non-repudiation*, could be achieved in a several ways. We must concentrate on the solution for all of them.

2.3. Background

Confidentiality is achieved through use of ciphers. Since the ancient times people used secret key cryptography to encipher the data they exchange. In this type of cryptography both sides in communication need to have a piece of information, the key, which enables decipherment. The problem with this system is that there must be a way, a secure channel, to distribute the same key to both sides in communication before communication over insecure channel can commence. This has become very impractical with development of modern telecommunications.

Then in 1976 Diffie and Hellman in their seminal paper [2] noted that with public key cryptography one no longer needs a secure channel over which to transmit secret key between communicants. They showed that a user could have two keys, private and public, that are mathematically related in such a fashion that revealing a public key does endanger secrecy of private key. It is actually possible, but computationally infeasible to calculate private key from a public one. For a secure communication data is encrypted with public key and can only be decrypted with private key. Public key can be sent to people one wants to communicate with or published in some sort of address book. In addition to confidentiality, public key cryptography could also provide authentication and non-repudiation. Only the owner of private key can encrypt the messages that can be decrypted with corresponding public key. This removes any doubt of message origin and prevents its creator from denying authorship. Digital signatures are created using public cryptography as well, but with little help of hash functions. Hash functions take a message, or any data, as its input and give unique, for given input, pattern of bits of predefined length as its output. Even single bit change in input data significantly changes output pattern of bits. A message that needs to be digitally signed is passed through hash function that creates so called message digest. Message digest is then encrypted with sender's private key. This encrypted digest is a digital signature that is appended to the message itself. This ensures data integrity and senders authentication. Any changes to message in transport would immediately produce different digest from the one in digital signature. Only the sender's public key could be used to decrypt digital signature what confirms the identity of sender. There are several different methods, mathematical functions, used in public key cryptography and hash functions but they all work on the above-described principles.

The weakest link in public key cryptography is public key distribution. One needs to be sure that published public key indeed belongs to the person the address book says it does. If the address book has been tampered with we might end up sending confidential message encrypted with public key of someone who switched entries in address book. In this case instead of intended recipient someone else will have access to our confidential data. Two years after historical Diffie-Hellman paper Kohnfelder, in his MIT bachelor's thesis [3] introduced term certificate as a digitally signed piece of information that binds a public key with a person it belongs to. Now, instead of looking up someone's public key, we look up his certificate that has been signed by someone everybody trusts and we might be sure that the public key that is part of the certificate is correct. The authority that signs the certificates is called Certificate Authority (CA).

2.4. Current PKI state

Certificate authority is one of the core components of a public key infrastructure. Other core components are:
- The End-Entities (EE)
- The Certificate Repository (CR)

• The Registration Authority (RA)
• Digital Certificates (X.509 V3)
The core PKI components and their relations are shown on figure 1.

A PKI offers the base of practical usage of public key cryptography. Originally, PKI was a generic term that meant a set of services that make use of public key cryptography. PKI has been exploited in many applications or protocols, such as Secure Sockets Layer (SSL), Secure Multimedia Internet Mail Extensions (S/MIME), IP Security (IPSec), Secure Electronic Transactions (SET), and Pretty Good Privacy (PGP). On the other hand, X.509 V3 digital certificate exploitation within PKI has been one of the most desired standardization issues in e-commerce. Since 1995, the Internet Engineering Task Force (IETF) PKIX working group started to fully involve X.509 V3 certificates into the PKI standards and make PKI worthy of practical use for critical business on the Internet. [4] The IETF PKIX working group standard is generally considered to be most widely accepted.

PKI, at least in theory, seems to be a good solution. In practice, number of implemented PKIs was much smaller then expected. There are two main reasons. First one being high complexity of practical implementations of PKI, and the other high cost of building or purchasing PKI system [5]. An average PKI solution costs 750,000 EUR. Large companies may pay substantially more – easily several million dollars. And if an organization wants to outsource putting a PKI solution in place, this can easily cost 50 USD per seat or more. [6]

3. SUGGESTED APPROACH

We defined what we want to achieve. We named security services we need. After little historical background current PKI state was presented. Conclusion so far might be that PKI is promising but hard to implement. This should not prevent us from building PKI at ETF. The benefits from PKI are big; we just need to make sure that implementation cost is not bigger.

There are several decisions that have to be made at the very beginning. Our school cannot afford above stated cost of PKI solution. Purchase of PKI system from big vendor or hiring an outside firm to implement it is not an option. We need to do some in house development combined with available and affordable products. At this point I will not go into any technical details but I will focus on some of the obstacles to implementing PKI and how to overcome them in our case.

3.1. Core components

First of all, we need to have core components of PKI.

3.1.1 Certificate Authority

Certificate Authority is the signer of the certificates. The logical domain in which a CA issues and manages certificates is called *security domain*. A CAs primary operations include certificate issuance, certificate renewal, and certificate revocation. [7]. Our security domain should be our school. There should be only one top ETF SA CA with no certificate chains. This CA's certificate would be self-signed. Software applications for CA implementation are part of IBM Domino and Microsoft Windows 2000/2003 that we have at ETF. There are also open source implementations that should be considered.

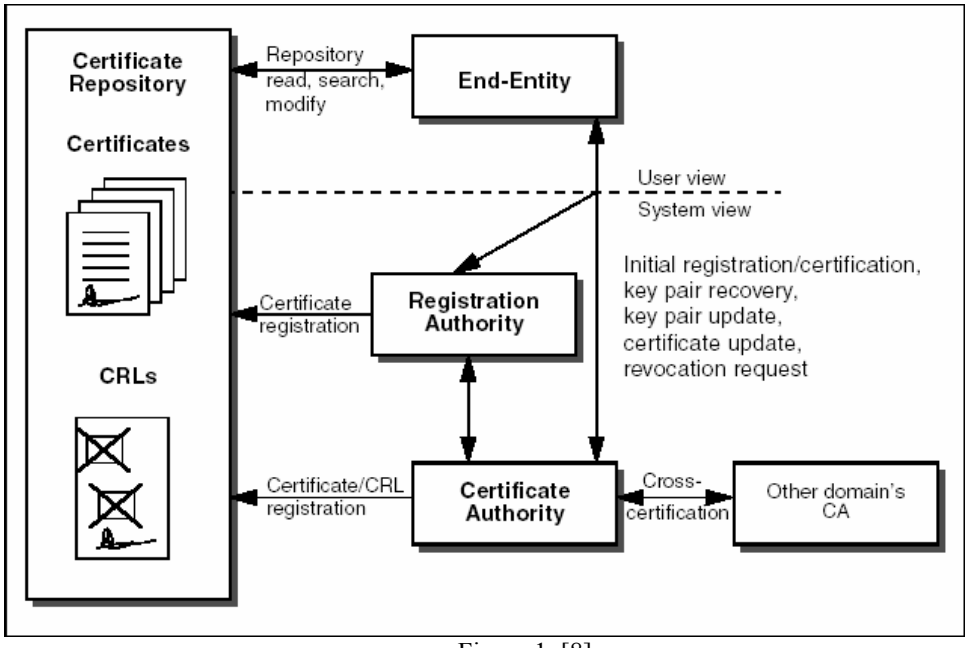

Figure 1. [8]

3.1.2 End Entity

An *End-Entity* is defined as a user of PKI certificates and/or end-user system that is the subject of a certificate [9]. In other words, in a PKI system, End-Entity is a generic term for a subject that uses some services or functions of the PKI system, which may be a certificate owner, or a requestor for certificate or CRL. In the beginning our End Entities will be school employees and students and ETF servers.

3.1.3 Certificate Repository

The Certificate Repository (CR) is a system or collection of distributed systems that store certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities [9]. Although a CR is not a required component in a PKI system, it significantly contributes to the availability and manageability of a PKI system. Because the X.509 certificate format is a natural fit to an X.500 directory, a CR is best implemented as a directory and it can then be accessed by the dominant Directory Access Protocol, the Lightweight Directory Access Protocol (LDAP) [10]. LDAP is supported by many applications and included as a part of some operating system suits like Microsoft Active Directory. Centralized, universal directories based on LDAP are being deployed throughout most organizations and certificates are just one of the objects served by such directory services. Similar to CA implementation, we can use IBM Domino or Microsoft Windows 2000/2003 implementations of LDAP, as well as an open source application.

3.1.4 Registration Authority

The Registration Authority (RA) is an optional component in a PKI. In some cases, the CA incorporates the role of an RA. Where a separate RA is used, the RA is a trusted End-Entity certified by the CA, acting as a subordinate server of the CA. The CA can delegate some of its management functions to the RA. [9] For example, the RA may perform personal authentication tasks, report revoked certificates, generate keys, or archive key pairs. The RA, however, does not issue certificates or CRLs. Our RA should be part of CA and use existing school infrastructure. This will be explained later when certificate issuance is described.

3.1.5 Digital Certificates

X.509 is the most widely used certificate format for PKI, being used in major PKI-enabled protocols and applications, such as SSL, IPSec, S/MIME, Privacy Enhanced Mail (PEM), or SET. A rare example of one that does not support X.509 certificate format is Pretty Good Privacy (PGP), which uses its own certificate format. Figure 2 is a basic structure of an X.509 certificate. Initially, X.509 v1 appeared in 1988 as ITU-T definition. X.509 v2 supports new fields over Version 1; they are *issuer* and *subject identifier*. The latest X.509 V3 was defined in 1996, which introduced the *extension* field. Currently, many PKI deployment applications are based on X.509 v1 or v2, but the PKI technology direction trends clearly to X.509 v3 based implementation. [11] We clearly need to use X.509 V3 in our implementation. Suggested CA implementing applications supports this format.

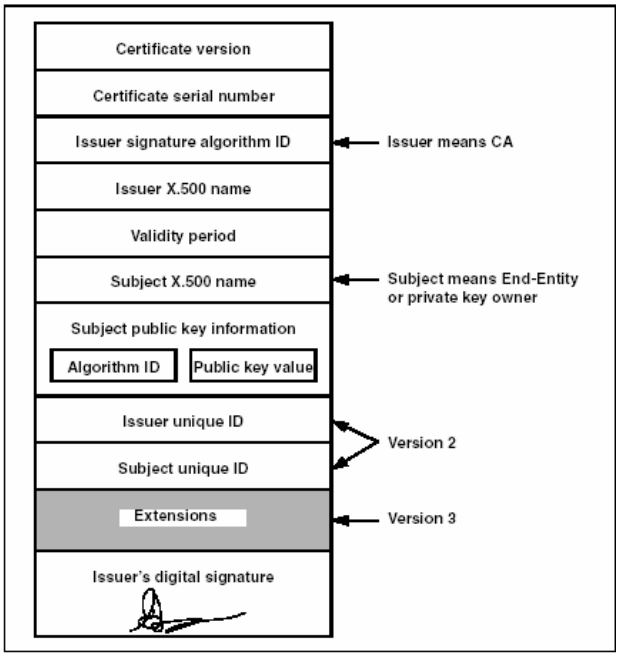

Figure 2. [8]

3.2. The supporting components

3.2.1 Certificate Revocation Lists (CRLs)

Certificate Revocation List (CRL) is one of two common methods for publishing list of revoked certificates along with reasons for revocation. The other, newer method, which has superseded CRL in some cases, is Online Certificate Status Protocol (OCSP). There are three ways a CA can publish a CRL [9]:

- Pull method - This method relies on the certificate-using application to periodically check recognized repositories or the latest CRL update. The CRL can then be "pulled" down for use by the application. The application can check certificate validity depending on the next scheduled update that will be published in the CRL. A CRL will be signed by the appropriate CA before being placed in the repository.
- Push method - This method relies on the CA broadcasting a CRL to certificate-using applications every time a certificate has been revoked. The CRL is "pushed" to applications.
- Online verification - This method requires the certificate-using application to execute an online

query with a particular CA before validating a certificate.

In a closed community, like our school, with predictable number of users that does not change much during school year suggested LDAP Certificate Repository with online CRL verification is a best solution.

3.3. Administration

Interactions among core PKI components, as shown on figure 1, tend to be the most difficult to implement. This is where our existing infrastructure and administration could be used to our benefit. Our existing administration procedures could be integrated or enriched with PKI administration procedures.

Process of initial registration and certificate issuance starts when End Entity makes itself known to RA or CA. End Entity positive identity verification must be performed before any further actions are taken. This tends to be a complicated task and some big PKI vendors, like VeriSign, have several different certificates depending on the level of confidence in user's identity. There is also an issue of private and public key generation. Key pair could be generated by user or by CA. If a user generates key pair, then the public key is sent as a part of request for certificate issuance. This is, for some uses, considered a safer option since the private key does not to be transferred anywhere, but requires clients that can generate key pairs. If CA generates key pair it needs to be securely given to a user together with a certificate. We could make certificate issuance process a part of our existing procedures. Students need to be positively identified during normal school enrolment procedure and can be issued certificates and given key pairs in person. Employees would be issued certificates and given key pairs when they are hired. Computer servers would get certificates when they are put online. All certificates would also be stored in a publicly available Certificate Repository.

User's private keys are sometimes backed by system. This enables lost key recovery. There is also an issue of privacy and responsibility for protecting backup copies of private key. The decision whether key escrow should be implemented is based on the value of the key, or to be more precise on the value of data encrypted and signed with this key. Therefore only CA, server and management keys should be backed up in a very secure manner.

Since certificates have validity periods they need to be renewed periodically. This could be made a part of yearly enrolment process for students and contract extension signing for employees.

In case of a situation requiring certificate revocation certificate user or authorized person informs CA who will put a certificate on CLR.

Key pair update should be very seldom-used operation. Update is needed if a private key has been compromised or lost and it is not backed up. It requires old certificate revocation and issuance of new one and can be covered with these two procedures.

Access to Certificate Repository enables RA and CA to register certificates and put them on CLR if needed. End Entities access CR to look up certificates of other End Entities and check their status. If CR is implemented as LDAP it then can be accessed with LDAP commands or procedures.

Cross-certification is mutual certification of two CAs residing in two different security domains. In the process of initial ETF PKI implementation there will be only one security domain but we should have procedure ready to cross-certificate CAs from other schools, universities, or any other entity we deal with.

3.4. Applications

Applications exploitation of PKIX standards is vital for the deployment of a PKI. Applications include high-level applications, such as Lotus Notes groupware, or some low-level security enablers, such as SSL or SET. Some everyday applications, such as the popular Web browsers from Netscape Communications Corp. or Microsoft Corp., already support a PKI to some extent. For example, a Web browser supports client certificate authentication using either built-in certificate storage or external Smartcard support. Popular mail client software supports signing and encrypting e-mail messages through the use of PKI features. It is easy to imagine that many new applications will soon exploit the PKIX standard. As a matter of fact, by using existing shrink-wrapped software for Web access and e-mail, organizations can make use of a PKI as of today. By using certificate authentication for application clients running in a Web browser and secure e-mail, many of today's business processes can already be incorporated into a PKI. [8]

This support for PKI already built in Web browsers and mail clients can be directly used to enable meeting most of our immediate needs stated in 2.1 above. Secure and controlled access to documents can be realized through Web browser by using secure HTTP (HTTPS) protocol based on SSL. Web pages with confidential data with limited access would require user to present a certificate in order to be served the page. User's certificate would be used to authenticate him and check if he is authorized for access. Server's certificate would assure user that he is dealing with ETF server. SSL would provide data confidentiality. Digital signatures would enable date publishers to guaranty data integrity and would also provide for non-repudiation. Future application should be built to use PKI, but even without them PKI could be effectively used to satisfy our immediate needs.

4. LEGAL CONSIDERATIONS

If we are to implement and use PKI we must define if and how legally binding digitally signed documents are. Only legal regulations in Bosnia that deal with this area are two Central bank decisions, both from year 2002. One regulates rules for establishing elements of qualified digital signature [12]. It makes digital signature legally equal to handwritten signature if the signature was created using digital certificate issued by qualified Certificate Authority. The other decision defines conditions for becoming qualified CA [1]. So far no CA has qualified.

It is important to say that [1] talks about digital signatures for money transactions, since it is Central Bank decision. ETF PKI system is not primarily intended for signing money transactions, but it should comply with applicable requirements set forth in [1] because it is the only legal definition of digital signature and CA. So, let us take a closer look at Central bank requirements defined in [1]. We need to see how we could meet them.

Some of the requirements are generic and some are more specific. By generic I mean requirements that are difficult to check. Therefore, I will show how our suggested approach complies with specific requirements and how it implicitly complies with generic ones.

The first and most generic requirement is for CA to provide all elements needed for issuance of qualified electronic certificate. This in fact requires creation of PKI and not only CA, and that is exactly what we intend to do.

There are several requirements that talk about secure storing and displaying lists of valid and canceled certificates with information on their validity periods. The Certificate Repository that we plan to build based on LDAP, if properly configured, meets all of the requirements.

Two requirements ask for positive identification of certificate owner and any other owner specific attribute, as well as informing owner about conditions for certificate usage. Our planned registration and certification process comply with those requirements.

There is a requirement for logging any PKI-related activity and safekeeping records for a specified period of time, especially for legal purposes. This is usually called auditing and is standard part of any PKI implementation, although it was not specifically mentioned before.

Several remaining requirements deal with ensuring adequate security measures are taken to prevent certificate from being compromised. This includes employing qualified personnel and using verified systems and products. These requirements can be checked only after all implementation details are known. For this reason we should keep them in mind in our future development efforts.

There is one more requirement that states that CA has to have enough financial resources to provide for safe and secure operation. This one might be the most difficult to meet for an educational institution.

Requirements for a digital certificate to be qualified are very similar to definition of certificate format X.509 V3 [11]. So if we use X.509 V3 certificates we would meet Central bank requirements for the elements of digital certificate.

It can be seen that complying with prevailing PKI standards will bring our PKI implementation very close to meeting Central Bank requirements for becoming qualified CA. There are some finer details of implementation that need to be taken in consideration in our future steps.

Apart from Central Bank, ETF can have its internal regulations that define validity of documents signed by ETF issued digital certificates. Massachusetts Institute of Technology is an example of school that issues its own certificates for internal use [13]. As it was said at the beginning we need to define what we need and what we are going to use digital identities for.

5. CONCLUSION

Public key infrastructure is a promising solution for an organization security needs but it is hard to implement. Approach suggested here offers an idea how working PKI could be implemented at an educational institution. The fact that a school is a closed community with predictable number of users that does not change much during school year is used to our benefit. By using existing features of already available software at school or open source software solutions to implement PKI components most of the expenses usually associated with PKI implementation could be avoided. Integration of PKI administration and management with existing school administration processes makes usually complex task of introducing PKI in an organization much easier. Support for PKI already built in Web browsers and mail clients can be used to satisfy most of immediate needs for secure communications. Suggested approach is also in line with current legal developments in the area of digital signatures and should result in legally binding electronic documents.

This is just first step in PKI implementation, but should be the most important and most difficult to make. Next steps should be to define security policy and then the technical details of implementation that should follow.

References

[1] Centralna Banka Bosne i Hercegovine, ”Odluka o minimalnim uvjetima koje mora ispunjavati kvalificirano certifikaciono tijelo koje izdaje kvalificirane certifikate za elektronski potpis”, Službeni glasnik BiH, broj 10/02, 24.05.2002.

[2] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, November 1976, pp. 644-654.

[3] L. Kohnfelder, "Towards a Practical Public-key Cryptosystem", MIT S.B. Thesis, May. 1978.

[4] IETF PKIX working group http://www.ietf.org/html.charters/pkix-charter.html

[5] P. Doyle, S. Hanna, “Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage”, OASIS Public Key Infrastructure (PKI) Technical Committee (TC), August 8, 2003, Version: 1.0

[6] Tech Spotlights “PKI Status: 2003” Infineon Technologies AG http://www.silicontrust.com/background/sp_pki2003.asp

[7] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC2510, IETF PKIX, March 1999

[8] H. Johner, S. Fujiwara, A. S. Yeung, A. Stephanou, J. Whitmore “Deploying a Public Key Infrastructure”, IBM Redbook, February 2000

[9] R. Housley, W. Ford, W. Polk, D. Solo,"Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, IETF PKIX, January 1999

[10] S. Boeyen, T. Howes, P. Richard, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", RFC2587, IETF PKIX, June 1999

[11] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

[12] Centralna Banka Bosne i Hercegovine, ”Odluka o reguliranju pravila za utvrđivanje elemenata za vjerodostojnost elektronskog potpisa”, Službeni glasnik BiH, broj 10/02, 24.05.2002.

[13] Massachusetts Institute of Technology - Information Systems, “Certificates at MIT”, http://web.mit.edu/is/topics/certificates/