Security Lane of the Road of IT towards Public Services

S. Mrdovic
University of Sarajevo / Faculty of Electrical Engineering, Sarajevo, Bosnia and Herzegovina
sasa.mrdovic@etf.unsa.ba

***Abstract*—This paper presents possible path for securing public IT services. Public sector IT services deployment issues are presented. Security needs are defined. Possible gains from ICT in public sector are quoted. Simple services with highest impact that should be secured and offered are defined. Public key infrastructure (PKI) is proposed as basis of solution. 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 public institutions are used to propose custom made PKI. Given approach lowers the cost and level of complexity of building PKI and brings them within reach of a public institution. Legal consequences of PKI implementation are examined.**

I. Introduction

Information and Communication technologies bring new opportunities for business development everywhere. SEE region could be the one to gain the most from current developments. There are lot of young educated people ready to embrace and implement new technology and a number of possibilities for new companies to be created and for old to be modernized using ICT.

One of the current issues that might slow down inclusion of ICT into business processes in SEE region is lack of trust and confidence in ICT. The fact is that big percentage of decision makers in SEE belong to generation that was introduced to computers and ICT technologies long after they finished formal education. For this reason we still have certain resistance to full introduction of latest ICT achievements, especially if it means sending data electronically over the Internet. Business owners and managers still fear that data might be somehow seen, altered or stolen while on “wires” or even worse while they travel through the air “wirelessly”.

While businesses will have to embrace IT in order to survive competition, public sector is not under such pressure. Public institutions might be even more hesitant to embrace new technologies. Even when they provide IT services to public they might not put that much emphasis on security of IT services. There are several reasons for this but two of them are cost and perceived complexity of implementing security.

Aim of this paper is to show that implementation of secure IT solutions does not have to be hard and costly and that they provide good return on investment.

II. Security needs

Computer security rests on confidentiality, integrity, and availability. Confidentiality is the concealment of information or resources. Access control mechanisms support confidentiality. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. [1]

Required level of system security is achieved through security mechanisms of prevention, detection and reaction (recovery). Prevention means that an attack will fail. Typically, prevention involves implementation of mechanisms that users cannot override and that are trusted to be implemented in a correct, unalterable way, so that the attacker cannot defeat the mechanism by changing it. Detection is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is under way, or has occurred, and report it. Recovery has two forms. The first is to stop an attack and to assess and repair any damage caused by that attack. In a second form of recovery, the system continues to function correctly while an attack is under way. [1]

Next, possible road to satisfy mentioned security needs within public IT services will be presented, with special emphasis on solution affordability.

III. ICT in public services

Now well known Gershon review [2] identified a potential of efficiency gains in the public sector of about 30 billion Euros by 2008. This source of gains produces resources that can be released for and contribute to socio-economic growth. The use of ICT in delivering public services can greatly contribute to greater efficiency and effectiveness as well as major savings, but these potentialities should be measured and should no longer be accepted as a given. The capability to measure the concrete impact of investment in ICT-enabled public services is therefore a strategic tool to both ensure accountability and monitor the actual realization of the promised benefits.

In spite all pros of ICT in public services, research report by The Work Foundation [3] points that skepticism remains about whether investment in ICT is worth the money and whether service delivery can be made demonstrably better. Information and communication technology (ICT) has the potential to transform the relationship between citizens and public services, and how public services are delivered – but only if it is clear what the ICT is being used for, and appropriate ICT is used to achieve these objectives. The public sector has not fully capitalized on the potential ICT offers – as the dependence on the Gershon recommendations for ICT demonstrates. One of the significant challenges of using ICT in public services that should not be overlooked are significant privacy issues raised by information sharing [3].

IV. Proposed solution

Privacy is achieved through more than technical IT solutions but technical part will be explained here. Citizen’s data privacy is ensured through previously explained security terms of confidentiality and integrity, if both of them are achieved than original, unaltered data is available only to those authorized to see them. There are a number of solutions to achieve confidentiality and integrity but almost all of them rely on cryptography. Cryptography provides the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems. [4]

Public services that could be offered using IT are numerous. Presenting security solutions for all of them would require books. Therefore one approach and ideas on its practical implementations will be considered. Of special interest are services with greater public exposure that satisfy needs of number of number of people. Good, that includes secure, implementations of such services present public institutions that offer them in best possible light and make future budget funding easier to get. Citizens, users of public service, should be able to use their computers to communicate in a secure fashion with public institution offering the service. Some of the services that secure implementation should offer are:

- The public institution need to be able to publish official signed public documents on its Web site
- The citizens need to be able apply for various documents and services online
- The citizens need to be able get documents and services, they are entitled to, online
- All users of the system need secure access to all the documents they are entitled to see

In order to be able to provide above services that are secure and legal, public institution must, among other things, be able to digitally sign documents it publishes and to allow its users, citizens, to do the same with applications citizens submit.

There is an idea for solution of secure public ICT services and it conveniently called Public Key Infrastructure (PKI). PKI is infrastructure that enables addition of security services to applications. Besides already mentioned data confidentiality and integrity, PKI could provide authentication, authorization and non-repudiation. Authentication requires users to prove that they are who they say they are. Authorization takes care that authenticated users can access only resources they are authorized to access. Non-repudiation guaranties that no side in electronic transaction can later deny its participation. [5]

PKI is not magic solution to all security issues. It is a good idea that might be complicated and expensive to implement. Several pointers on how to avoid those pitfalls will be given after some cryptography background of PKI.

A. *Cryptography 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 [6] 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 [7] 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).

B. *Public Key Infrastructure*

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. [9] The IETF PKIX working group standard is generally considered to be the most widely accepted.

PKI, at least in theory, seems to be a good solution. In practice, number of implemented PKIs was much smaller than expected. There are two main reasons. First one is high complexity of practical implementations of PKI, and the other one is high cost of building or purchasing PKI system [10]. 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. [11]

V. IMPLEMENTATION

After basic cryptographic and PKI terms are explained and current PKI state is presented, it is time to suggest ways to implement practical PKI. The benefits from PKI are big; institutions planning on using it just need to make sure that implementation cost is not bigger.

Most public institutions cannot afford above stated cost of PKI solution. Purchase of PKI system from big vendor or hiring an outside firm to implement it, usually is not an option. Solution might be in some in house development by institution's own or temporary outsourced IT staff combined with available and affordable products. PKI components do not have to be expensive to acquire and deploy. A number of them come as a part of existing software or have free available open source version, as it will be presented.

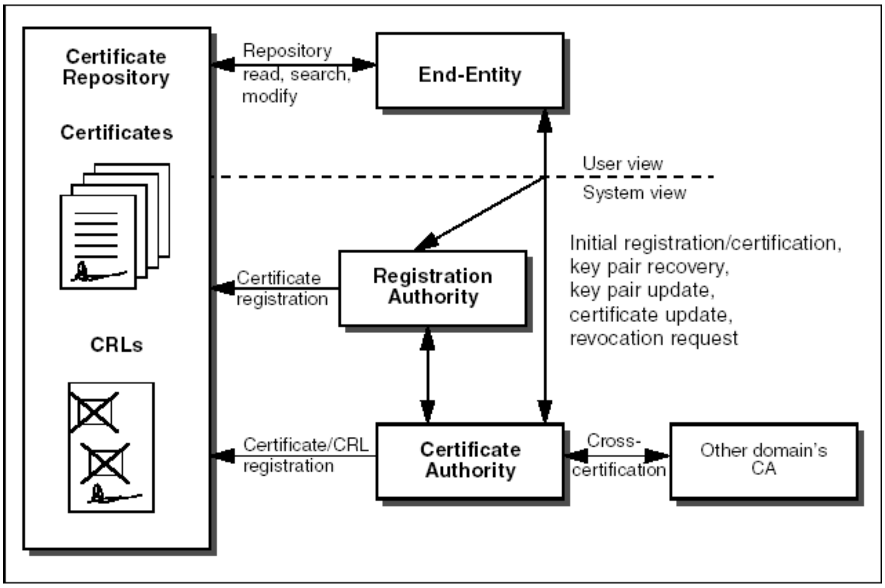

Figure 1. The core PKI components and their relations [8]

When deploying a PKI, the most important part is appropriate CA software. There are several solutions on the market:

- Microsoft: Windows 2000 Server and Server 2003 contain CA software, which is integrated into the Active Directory. It doesn't cost additional license fees. This is currently the most popular solution on the market.
- Linux: Linux supports OpenSSL and OpenCA, which are two freeware CA solutions.

Either solution does not require any investment in purchasing new software. Both solutions are well documented and easy enough to deploy. Besides those, there are number of free and open source CA implementations like “Mozilla Open Source PKI Projects” [12], OpenXPKI [13].

CA is the heart of PKI, but other PKI components need careful consideration. End entities in this PKI are citizens, users of services, as well as public institution employees and computer servers. 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. 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). 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. Public institution should its existing Directory Service as Certificate Repository. Registration Authority registers users and is an optional component that can be implemented as a part of CA. 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. It is an obvious choice for public institution deploying PKI.

Interactions among core PKI components, as shown on figure 1, tend to be the most difficult to implement. This is where public institutions existing infrastructure and administration could be used to its benefit. 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. Public institution could make certificate issuance process a part of existing procedures. Citizens need to be positively identified during voting or similar registration and can be issued certificates and given key pairs in person at that time.

Applications exploitation of PKI standards is vital for the deployment of a PKI. Applications include high-level applications, such as 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. [14]

This support for PKI already built in Web browsers and mail clients can be directly used to immediately enable secure implementation of services described as most needed in proposed solution. 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 public institutions 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 proposed PKI could be effectively used to satisfy immediate needs.

It is important to mention that PKI has support in legal documents. There is Directive of the European Parliament and of the Council on a Community framework for electronic signatures [15]. The main provision of the Directive states that an advanced electronic signature based on a qualified certificate satisfies the same legal requirements as a handwritten signature. It is also admissible as evidence in legal proceedings. According to Commission report [16] from 2006 on the operation of Directive, all the EU Member States have implemented the general principles of the Directive. It is noted that transposition of the Directive into the legislation of the Member States has met the need for the legal recognition of electronic signatures. Report also concludes that there has been far less use of qualified electronic signatures than expected. The main reason for this is economic, in that service providers have little incentive to develop a multi-application electronic signature and prefer to offer solutions for their own services. A number of applications in the future might nonetheless trigger market growth, particularly in relation to eGovernment services.

VI. Conclusion

ICT offers potential for huge efficiency gains in public services. One of the issues that are slowing down deployment of ICT is security. Basic security requirements need to be met for IT service to be useful. Ability to digitally sign electronic documents would give boost to number of applications. Digital signatures are well known technology, but are seldom used by public institutions. Public Key Infrastructure provides infrastructure for digital signatures and other needed security services. PKI deployment might be expensive and complex, but it does not have to be. This paper presented cryptography background and PKI components. It also suggested how PKI can be built with readily available and affordable blocks that might already be in use in public institution. Legal status of digital signature is explained.

References

[1] M. Bishop, "Introduction to Computer Security", Addison-Wesley Professional, 2004

[2] P. Gershon, “Releasing Resources for the Frontline: Independent Review of Public Sector Efficiency”, 2004.

[3] A. Jones, L. Williams, "Public services and ICT - final report. How can ICT help improve quality, choice and efficiency in public service? ", Research report, The Work Foundation, 2005.

[4] R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley, 2001

[5] A. Menezes, P. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.

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

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

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

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

[10] 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

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

[12] Mozilla Open Source PKI Projects Web Site http://www.mozilla.org/projects/security/pki/

[13] OpenXPKI Project Web Site http://www.openxpki.org/

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

[15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p.12.

[16] Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, Commission Of The European Communities, COM(2006) 120 final, Brussels, 15.3.2006