PKI USAGE ON ALBANIAN GOVERNMENT – LEVEL INFRASTRUCTURE PROJECTS

Marin Aranitasi[1], Marsida Ibro[2,] Enida Sheme[3]

[1]Center for R&D, Polytechnic University of Tirana, maranitasi@fti.edu.al
[2] Department of Telecommunication and Electronics, Polytechnic University of Tirana, marsida.ibro@gmail.com
[3]Department of Computer Science, Polytechnic University of Tirana, esheme@fti.edu.al

Abstract

Perhaps one of the most critical elements of security is the ability to provide trust to the electronic transactions. One technology that helps injecting trust and confidence to these transactions is Public Key Infrastructure (PKI). Today, PKI has been viewed as critical and necessary not only to the commercial sector but also to the government sector.
The purpose of this paper is the design and implementation of a government electronic system, which will increase the digital identity management security of its users. We will focus on the Albanian business users (from small companies to big corporations). The proposed solution was achieved after the consultation with different national security projects. We consider also the environmental characteristics of these projects and adapted them to our standards.

Keywords: *e-Government, Digital Certificate, Albania, Security, Cryptosystem*

1. Introduction

The today world is totally dependent from e-commerce. Internet is the most common and effective tool to increase the internet transactions. Someone will say that we have the tools for affording trust to internet. But this is not totally true. For example anti-viruses and firewalls do not help in establishing the identity of the parties during transactions. Also these solutions do not help in the understanding of the level of trust when we are doing an online transaction or dealing with an individual So we need a method or a technology to provide trust and confidence to the internet. Some of the few technologies that can accomplish this include ***Public Key Infrastructure (PKI)***. For a lot of people, PKI includes complex and long deployments. Perhaps this may have been real a few years ago, but today is different. As we mentioned before, PKI has been viewed as a critical and very necessary not only to the private sector, but also to the government sector. A lot of countries, within the last few years have passed laws that make digital signatures legally equivalent to physically drafted signatures. In addition, many countries also have some regulatory elements to the Certificate Authorities to ensure the quality of their operations. In the second section we will analyze the problems that have the Albanian government these days. In the third section we mention some of the national PKI government projects that we take into consideration. In section 4 we give our schematic solution and in section 5 we explain our detailed scheme. Section 6 describes the concrete PKI infrastructure that we implemented. In section 7 we present our future plans and in section 8 are the conclusions.

2. Problem description

The government services are divided in three major groups:

1. Government to Citizens (G2C)
2. Government to Business (G2B)
3. Government to Government (G2G)

Actually in Albania the Government to Business group of services is operational. Each of these services has their respective web sites. This is a good thing, but there is a problem with the number of websites addresses to remember. Also the users have to remember the credential for accessing each web site. This is quite impossible. The problems can be summarized as follows:

1. Users have to remember a lot of identification elements
2. Users in case of a lost or in case they forget the id elements, have to go to the specific institution, with an official request, to get back their id information.
3. Every institution has to create help desk structures that in 80-90% face with issuance of id elements.
4. This mechanism of management has big problems, because we can't guarantee the authenticity of the operations with the electronics services, if the credentials are so "OPEN".

We can divide these problems in two main categories:

1. **Citizen problems:** waste of time, going from one institution to another, waiting, and probably not solving the problem in time.
2. **Institution problems:** have increased costs :
   - The institution that gives the information has paper and printing costs, because the electronic information must be printed.
   - The institution that accepts the information has equipment costs, because the information is in paper format and needs to be entered in the system.

The objective of this project is:

To design an electronic communication infrastructure between the electronic systems of the different institutions, that allows the online identification of their users.

3. Related Work

There are many government initiatives that are based on PKI. According to [1] one of the biggest government PKI-based projects in the United States is "Common Access Card (CAC)", developed by the Department of Defense (DoD). CAC holds specific information and applications on PKI certificates, for the particular needs of the department. From the perspective of PKI, one of the CAC smart card holds up to three certificates to keep personnel information.

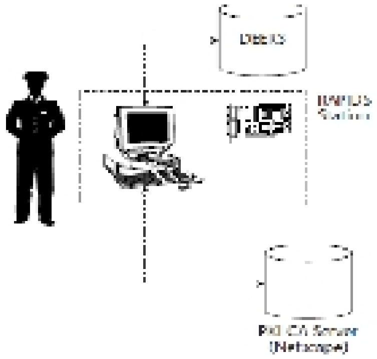

Figure 1. CAC

Three certificates stored in the CAC include:

1. **An authentication certificate**. This certification is reserved for transactions. Specifically in this certificate is used to sign documents and to access secure DoD Web portals.
2. **A signature certificate**. This certificate is used to sign e-mail.
3. **An encryption certificate**. The certificate is used by others to send encrypted e-mail to users of CAC card.

In the following chart we see the dependencies between the authentication and price.

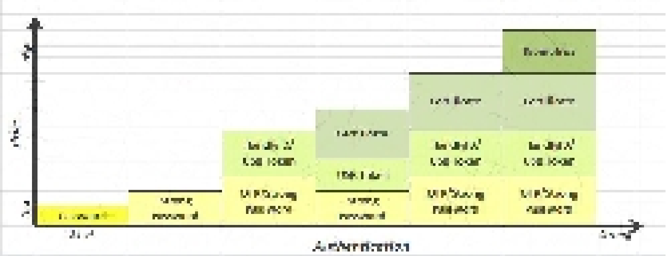

Figure 2. Authentication vs Price

As seen from this graph identification technologies begin to be confident when starting to use "authentication with two elements".
Another project that we take into consideration is the South Korean national PKI project [15].

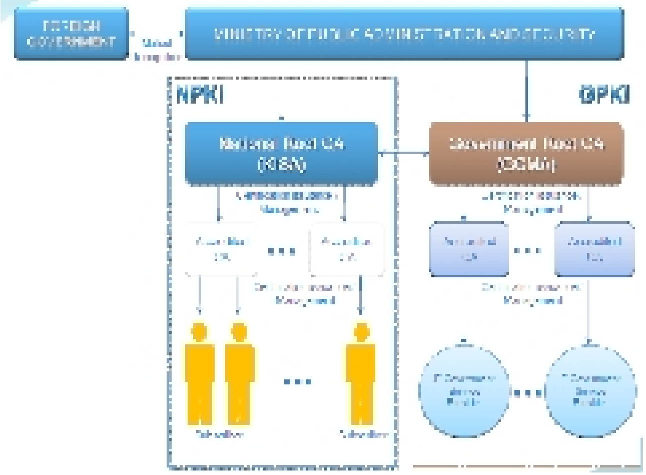

Figure 3. South Korean National PKI project

These projects show scalability and reliability under extreme environmental conditions such as high security, with a very large population.

4. Schematic Solution

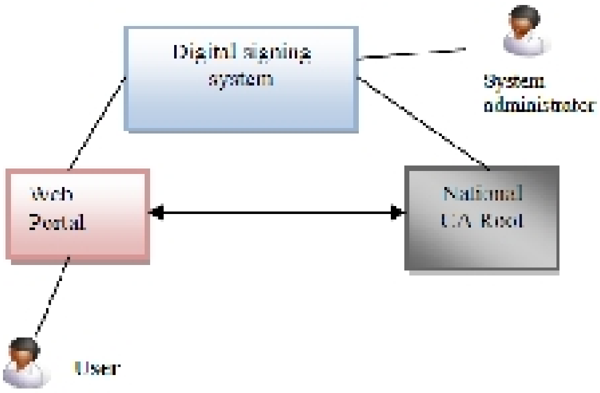

Figure 4. Schematic solution

The explanation of terms in the above chart is as follows:

- **The user –** the service user
- **SCDev -** the equipment that contain the citizen electronic identity and digital signature.
- **Web portal**. Portal in which the services are offered on-line.
- **National Root CA**. Built a PKI infrastructure which issues certificates for electronic signature. This infrastructure also publishes the CRL list (list without valid certificates) which is used for OCSP service.

Also this infrastructure will provide TSP service.

- **OCSP**. Online Certificate Status Protocol [2]
- **TSP** - Time stamping.[8]
- **CRL**. Certificate Revocation List[14]
- **E-Signature System**. The application that signs the document (including the processes for determining the validity and time stamp).
- **The system administrator**. Person responsible for the administration of the system.

So we need to get into more detail to explain our solution.

5. Hardware architecture of the solution

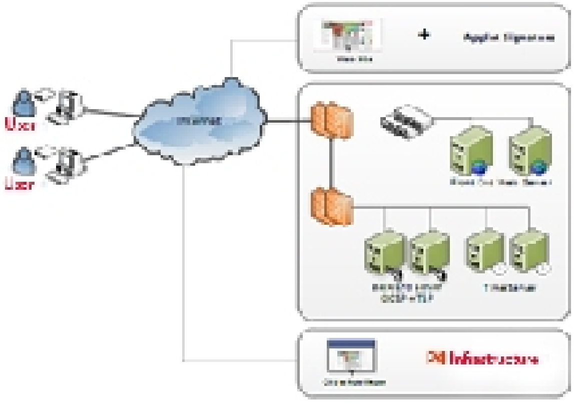

Figure 5. Hardware architecture

Based on the not very large number of signatures that will be realized in the first year of implementation, in order to have an acceptable economic solution, we decided that we will implement OCSP and TSP services on the same server. This solution is also provided with full redundancy in each of the components. Also the solution is conceived to be scalable in each of its components, in order to handle the increasing number of requests for service.

The functional blocks of the system are:

- **Web Site**. This component is the portal in which will be uploaded the documents that need to signed electronically (e.g. procurement portal, tax portal, etc.). An application for signature must be installed in this portal. This application needs to integrate several of its components with the existing structure of the web-site
- **PKI infrastructure**. This is a PKI infrastructure of an existing or new CA that will be established. For our system is of primary importance to co operate with two components:
  - To have access to the published CRL list, which is used from OCSP system, to validate the certificate of the user.
  - To confirm the identity of the user (service requester).
- **OCSP / TSP**. This component of the system serves to implement the signature-based services (time stamp application and the application for validation and electronic signature). The system is designed with two levels (tier) of hardware. In the first level we have placed two Web Servers, after the firewalls that protect servers from the Internet and in load balance. In the second level we have placed 2 servers, to execute the OSCP and TSP applications. In each of the servers will be installed Hardware Security Module (HSM) and a local data base. We will install 2 time servers connected to a GPS antenna. These servers will provide the exact time that will be used for the TSP application.

6. Public Key Infrastructure

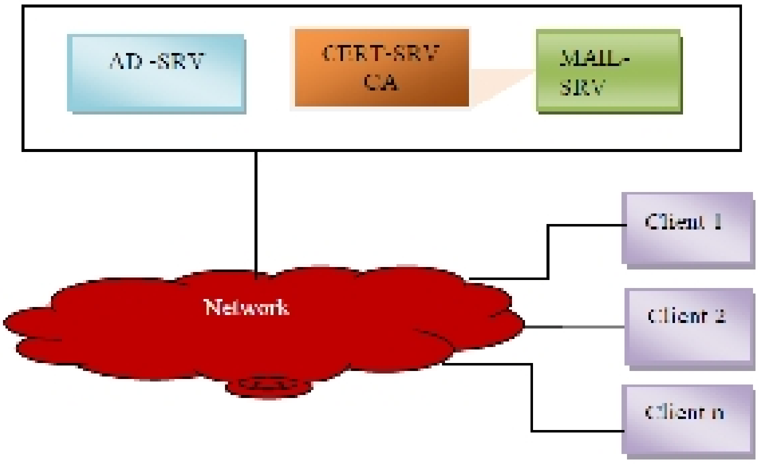

Figure 6. PKI

As given in Fig. 5, one of the three elements of the scheme is the PKI infrastructure. Fig. 6 shows one part of the project that is the PKI infrastructure. It consists of:

- Active directory Server (AD-SRV)
- Certificate Authority Server (CERT-SRV CA)

- Mail server (MAIL-SRV)
- Clients

All of these components were built in a government institution called AKSHI (National Agency of Information Society www.akshi.gov.al). We built an active directory and registered it to the ".gov.al" domain. Using [3][4][5][6][7][8] we set up our Certificate authority. We built also a mail server. We decide that our certification authority will issue two kinds of certificates.

- A login certificate
- A signing certificate

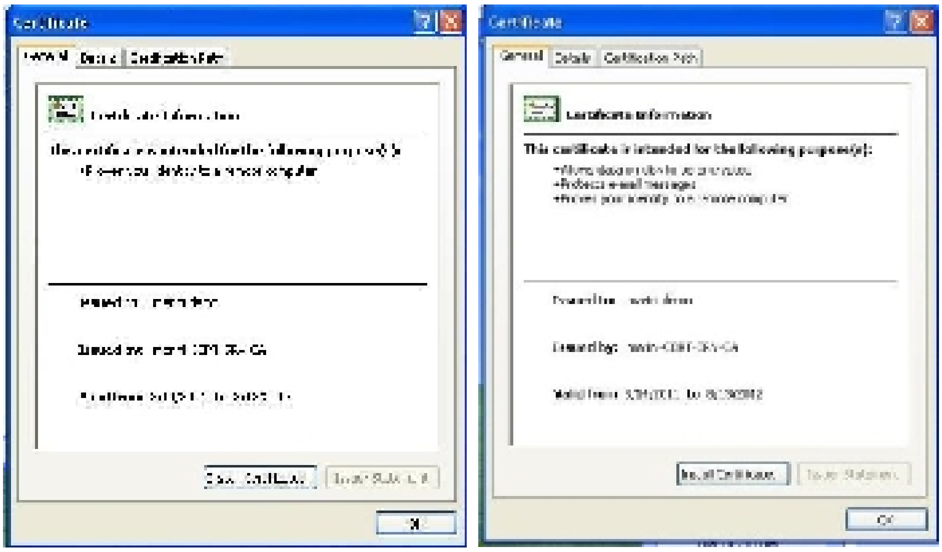

Figure 7. Digital Certificates

This picture shows two certificates that were generated in one of our tests and have a limited validity, only one month. To have a secure but not expensive system we decide to use as device that will keep the certificates of the users, a smart card. Each smart card needs a smart card reader to be used. With this smart card each user of the system can login only by putting his smart card into e reader. This mechanism simplifies a lot the logging process. We decide to issue only two types of certificates because the services that are now operational are focused only on digital signing and remote login in to the system. For security reasons we decide to set the time validity to one year.

7. Future Work

We divide the hardware solution in three individual projects. The first part, the PKI infrastructure is done successfully. The second (the OSCP&TS) and the third, the web site, are going to be implemented in these months. As we know the lightweight directory access protocol (LDAP) is the Internet standard way of accessing directory services that conform to the X.500 data model.[9] When implementing these projects we will take into consideration the deficiencies when LDAP is used to support PKI that were presented in [11]. We suppose that we will use the new method proposed in [12][13]. Also we will take into consideration the problems between different PKI implementations and the solution given to these problems by [16]. In the end we are going to implement the web site that will be the interface between the users and the system. Details of these implementations we are going to present in another paper.

8. Conclusions

We saw in this paper the problems that have actually the Albanian government in the process of digitalization of their processes and the identification of their users. To solve these problems we propose to build a PKI infrastructure. But this infrastructure was adapted to our standards. Today in Albania the group services that are available is the government to business. This group needs to send and receive secure documents with the government institutions. We presented our conceptual solution and then we present our detailed solution. The scheme of solution was divided into three little projects. The first was the set up of the PKI infrastructure. We set up this infrastructure. The core of it is the CA certification authority. Also we decide to issue two types of certificates the login certificate and the signing certificate that electronically signs the documents and e-mails of the business users. So the problem of identification of the users is solved. We need now to fully construct our system, i.e. to built the OCSP and TSP servers and integrate all of them into the web site. Now the Albanian government is a "little" more secure.

9. References

[1]Wiley - PKI Security Solutions for the Enterprise - Solving HIPAA, E-Paper Act, and Other Compliance Issues pp. 160-163 (2003)

[2]M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, Online certificate status protocol – OCSP, Internet Engineering Task Force: RFC 2560, June 1999.

[3]Open CA LibPKI, available at: https://www.openca.org/projects/libpki/.

[4]Open CA OCSPD, available at: https://www.openca.org/projects/ocspd/.

[5]Open CA project homepage, available at: https://www.openca.org/.

[6]Open SLP project, available at: http://www.openspl.org.

[7]Open SSL homepage, available at: http://www.openssl.org/.

[8]Open TSA available at: http://opentsa.org/

[9] Boeyen, S., Howes, T., Richard, P. "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2." RFC 2559, April 1999

[10]Wahl, M., Howes, T., Kille, S. "Lightweight Directory Access Protocol (v3)", RFC 4510 June 2006

[11] "Deficiencies in LDAP when used to support Public Key Infrastructures" David Chadwick, University of Salford, Salford M5 4WT, England

[12]"A New On-line Certificate Validation Method using LDAP Component Matching Technology" Jong Hyuk Choi, Sang Seok Lim, and Kurt D. Zeilenga, (2005)

[13]“Design and Implementation of LDAP Component Matching for Flexible and Secure Certificate Access in PKI” Sang Seok Lim, Jong Hyuk Cho,i Kurt D. Zeilenga. (2005)

[14]Profiles of X.509 v3 Public Key Certificates and X.509 v2 Certificate Revocation Lists (CRLs) RFC 5280 May 2008

[15]“Overview of National PKI Establishment” Jaejung Kim 2009 www.sgco.kr

[16] Finding the PKI needles in the Internet haystack” Massimiliano Pala and Sean W. Smith, *Computer Science Department, Dartmouth College, Sudikoff, Hanover, NH, USA,* Journal of Computer Security, 2010