A PKI ARCHITECTURE USING OPEN SOURCE SOFTWARE FOR E-GOVERNMENT SERVICES IN ROMANIA

NICUŞOR VATRA

The Doctoral School Department,

The Bucharest Academy of Economic Studies, 6, Romana Square, district 1

Bucharest, 010374, Romania

nicusor.vatra@yahoo.com

http://doctorat.ase.ro

Abstract

This article presents an architecture based on Open Source software that promote citizen's access to electronic services in a secure way and attempt to make an analysis between two different Open Source Public Key Infrastructure software: OpenCA PKI and EJBCA.
The architecture represents a suitable solution for a large enterprise or public administration that enables security and easy management of electronic documents in e-Government Services area.

Keywords: - public key infrastructure, e-Government Services, Open Source, encryption, electronic signature.

1. Introduction

The recent technological developments such as extension of modern communication and particularly the Internet boom have made the electronic world to create brand new opportunities for realizing transactions on the Internet. Due to ease to use, flexibility but also lack of explicit rules and restrictions, the Internet has become the most popular platform and the most important communication channel for the electronic transactions.
One of the major characteristics of any electronic transactions performed on the Internet is trust. On the Internet, where there is no direct contact between 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 using Trusted Third Parties (TTPs) known as Certification Authorities (CAs) [1]. These digitally sign data structures named Public Key Certificates (PKCs), ensuring that a specific public key belong to a certain user. Thus, certificates and their keys give the connecting information about their organization partners. The recipient of a certificate has to confirm 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 the other's certificate 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 such a trust link named "Trust Models". These permit a user to create chains of certificates from its trusted CA to other users recognized as certification paths

2. Related work

Since the beginning of Open Source software has been and remains alternative to commercial software, in time has gained popularity and visibility in most private sectors and now we find in operating systems and office applications as well in dedicated applications such as Public Key Infrastructure. There are currently serious debates in use of such software in public administration in Romania and principal arguments that support its use are low cost of purchase (in some cases even inexistent), interoperability also an increased level in ensuring security. Main feature of Open Source software is the availability of source code that can be modified and adapted to the needs of those who want to use it and according with license which are distributed all types of software package including Open Source software that stipulate what you can do with that software, if you can redistribute to anyone or can be installed on many computers, etc. During this period when the economic crisis is felt in all sectors public administration should take into account the use of Open Source software as an alternative to the commercial software.

Before move with the types of services and the planned architecture, we list some of the successful Open Source PKI software.

- OpenSSL: is the most widely used protocol for secure network communications and became the most popular and effective Open Source version of SSL/TLS. The OpenSSL toolkit is based on the SSLeay library that was originally developed by Eric A. Young and Tim J. Hudson in Australia. OpenSSL provides an Open Source set of libraries and utilities that enables network applications to include SSL and TSL versions The OpenSSL toolkit provides a foundation for many other applications (e.g., Web servers, mail servers, and so on). At the time of this writing, the version is 1.0.0d.
- PHPki: PHPki Digital Certificate Authority is an Open Source Web application for managing a multi-agency PKI for HIPAA compliance. With it, you may create and centrally manage X.509 certificates for use with S/MIME enabled e-mail clients, SSL servers, and VPN applications.
- Cryptlib consists of a set of layered security services and associated programming interfaces that provide an integrated set of information and communications security capabilities. Much like the network reference model, cryptlib contains a series of layers that provide each level of abstraction, with higher layers building on the capabilities provided by the lower layers.
- OpenCA: officially the OpenCA PKI Research Labs and formerly the OpenCA Project, is a PKI collaborative effort to develop a robust, full-featured and Open Source out-of-the-box Certification Authority implementing the most used protocols with full-strength cryptography. At the time of this writing, the version is 1.1.0.
- EJBCA: is an enterprise class PKI Certificate Authority built on JEE technology. It is a robust, high performance, platform independent, flexible, and component based CA to be used stand-alone or integrated in other JEE applications

3. Public key infrastructure components and service

Public key infrastructures have turned out to be 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 [2].

Trust is an essential part of any type of communication, electronic or physics. In the physical communication, trust is relatively easy to achieve since can identify the individual seeing it in person or by identifying marks, as handwritten signatures. Still in the case of electronic communications trust in another entity can be tricky since their identity can be hidden and signs allow us to identify in real life are not available. The reliability between two entities cannot be initiated, unless both entities are sure of the identity of the other and the information they are giving through a network is not being modified in transmission. These difficulties are resolved in part by public key algorithms because we provide confidentiality and authentication, but we encounter a problem:

In what manner can we be certain that a public key actually belongs to the person with whom we are communicating? We need some method relates in some way, the identity of an entity in the real world with identity in the electronic world. To solve these problems of reliability, authentication and security communications stand up PKI's and digital certificates. A PKI provides security and real-world confidence in the electronic world.

Digital certificates are the key elements on any PKI's. Digital certificate is a document signed, generally public, which associates a key public identity. The identity may contain, for example, the name of a person or organization, its country of origin or email address. A digital certificate contains three key elements:

- The subject's public key;
- The subject identification data ;
- Digital signature of a third party who ensures that the two above items are related.

In a PKI certificate signature is performed by a trusted third party, which certifies the relationship between a real and an electronic identity.

3.1. *PKI components*

A PKI is a framework of people, processes, policies, protocols, hardware, and software used to generate, manage, store, deploy and revoke public key certificates.

Elements of a PKI include system components such as one or more Certification Authority, a certificate repository; documentation including Certificate Policy document, one or more Certification Practice Statements and trained personnel performing trusted roles to operate and maintain the system. PKI integrates digital certificates, public-key cryptography and Certification Authorities into total organization-wide network security architecture [4]. A representative organization PKI encompasses the issuance of digital certificates to individual users and servers; end-user registration software; integration with certificate directories; tools for managing, renewing and revoking certificates and related services and support.

The main elements of infrastructure are [5]:

- Certifying Authorities - basic component of a PKI to issue and revoke digital certificates;
- Registration Authorities - validates requests for issuing certificates and identity of end users;
- Repository - store and distribute certificates and certificate revocation lists (CRL), they are issued periodically by the CA and are lists of certificates that are no longer valid;
- Archives - an archive is responsible for long-term storage of information in the name of the certifying authority, certifying that the information archived it was good when that was received and was not changed while it archived;
- End Entity - are the end users or equipment’s for digital certificates that were issued.

3.2. *PKI service*

PKI facilitates storage and exchanges electronic data in a secure way, safety is ensured by using public key cryptography, the types of security services offered are [3]:

- Confidentiality - safekeeping the private nature of the message is achieved using the encryption and use the public key from a certificate to establish an encrypted communication channel is the outcome 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 changed, is obtained with the help of a digital signature and by verifying the signature successfully, that message has not been changed after signing.
- Authenticity - confirming the identity of an individual or an application which sends out 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 are an essential security condition and dates from ancient times.

4. Certification Authority: EJBCA and OpenCA

A Certification Authority is the essential component of a public key infrastructure and primary function is to issue and revoke certificates. These may be issued for different goals like validate users and devices, secure communication with SSL clients and servers, signature and email encryption, signing documents, access to systems by using cryptographic cards, secure VPN connections and many others.

Enterprise Java Bean Certificate Authority or EJBCA, is an Open Source public key infrastructure certificate authority software, the project was initiated by Tomas Gustavsson and Philip Vendil ten years ago, at the moment the project is maintained and sponsored by the PrimeKey Solutions a Swedish company, which holds the copyright to most of the codebase. The first public release was in 2001, and now after ten years the

current version of EJBCA is 4.0.1, is written in Java and can be installed o any operating system platform the source code of the project's is available under terms of the Lesser GNU General Public License.

EJBCA as is described in their official website is defined as a trusted certificate authority that is based on J2EE technology, CA is a robust, scalable, high performance, component-based, multifunctional. Is multifunctional because it can perform all the functions of a CA, and some more, not delegate them to other tools and based on components because each of the functions is performed by a component of the tool itself. This project provides an enterprise-level PKI solution that enables building a complete infrastructure for large enterprises and organizations.

OpenCA is another Open Source project started in 1998 that implements a robust certification authority, using the services provided by other Open Source applications as OpenLDAP, OpenSSL, Apache, etc. Availability of the code by keeping it "open" as possible so that all join forces community, both through providing their views and possible modifications, in this way it has a remarkable evolution based on feedback given by developers and users. Is developed in Pearl who was chosen for its simplicity and portability based on convention that security is not based in the darkness, so that the code is easily readable. The software provides a web interface through Apache web server, which can be used through a browser and allows performing operations provides the certifying authority: Applications, revocation, search certificates. The configuration of certification authorities in addition performed via a web interface. The application furthermore implements protocols certificate status check both online and offline services publication of certificates.

By his nature Open Source, OpenCA provides facilities to modify their functionality according to the requirements of each PKI. In addition, as acknowledged previously configuration process can be customized by the needs of the organization where is installed. In Table 1 we see a comparison between EJBCA and OpenCA considering different parameters.

Table 1. Comparison between EJBCA and OpenCA.

Parameter	OpenCA PKI	EJBCA
Operating system installation	Linux, Solaris, Mac OS X, BSD	OS Independent
Implementation	C, JavaScript, Perl, PL/SQL, Unix Shell.	Java
Modules	Perl	EJB
Browser	Multiple	Multiple
LDAP and OCSP support	Yes	Yes
Smart cards support	Yes	Yes
Algorithm	Can be chosen	Can be chosen
Database	PostgreSQL, MySQL, Oracle, DBM	MySQL, PostgreSQL,, Oracle, DB2, Derby, Sybase, Informix, Ingres
Scalability	Not so scalable	Scalable
Easy of configuration	Complex	Extremely complex
Licenses	BSD Revised	LGPL
Costs	Free	Free

Architecture of a PKI is composed of operational and security policies, security services and protocols that support interoperability using public key encryption and key management certificates [6]. There are three basic types of architectures composed according to the number of Certification Authorities (CA) on existing PKI. In a PKI digital certificate issued by CA and applications are usually processed by the Registration Authorities (RA), the responsibility of an RA is to analyze individual user who examines each application and notifies the CA, which is closer to the level of confidence of the applicant by checking the level of confidence, CA issue the certificate.

PKI Architectures [7]:

- Single CA is a CA that issues certificates to users and systems, but not to other CAs, is easy to build and manage, users trust it and paths have one certificate and one CRL and do not scale particularly well.
- Hierarchical PKI is the traditional building model; trust the same central root CA and all the CA have a single superior CA, except the exception of the root CA.
- Mesh PKI is the first alternative to a hierarchy, multiple CAs provide PKI services and the CAs are related trough per-to-per relationships, each user trust a single CA, certificates issued to CA in a mesh PKI are more complex than the ones usually found in a hierarchical PKI.

The operation of CAs and RAs are governed by appropriate policies, the Certificate Policy (CP) and the Certificate Practice Statement (CPS). The first provides rules for naming certificate holders, the cryptographic algorithms that will be used, the minimum allowable length of encryption keys, etc. The latter details how the Certification Authority will implement the Certificate Policy (CP) into its procedures.

5. Proposed architecture ROPKI

At this time in Romania are several PKI solutions carried out at the Ministry of Internal Affairs, Romanian DoD, Ministry of Public Finances and other Governmental offices must be interconnected to achieve documents exchange, so we need a flexible mechanism that linking them to be interoperable. This mechanism is called the Bridge Certification Authority (BCA); it was created to connect the different areas of PKI by establishing relationships of trust.

The objective of the national PKI that we plan to build is to facilitate exchange of information through this secure infrastructure. The main actors in this process will be state institutions (government) and citizens. Both the governmental employee and the citizen will have digital certificates, which they will use to communicate securely.

The governmental employee will receive a certificate from a specially created certification authority that signs certificates only for the governmental employees that work in a certain ministry or other governmental agency.

By establish a certification authority for every major governmental agency or ministry we can set up a nationwide public key infrastructure who will not have a unique point of failure, because each of these authorities will be a ROOT CA and trust will be constituted by cross – certifying each with the national Bridge CA.

Governmental CA's issue certificates only to users of government civil servants. Each citizen will have to acquire a certificate from private companies that offer certification services.

To acquire a trust link among public servants and so citizen and so enable any citizen to request public services from public institutions (like ministries and Government Departments and Agencies over the Internet, we require that the private certification authorities cross –certify, as well, with the national Bridge CA.

5.1. *RO-BCA components*

RO-BCA is composed of the following elements: certification authority, repository server (LDAP), OCSP server, time stamp server (TS) and this to ensure interoperability by setting up cross-certification links between public key infrastructure in the public administration and other agencies or private institutions.

5.2. *ROPKI software solution*

The intended software for the construction of RO-PKI it will be Open Source software: OpenSSL used to create, sign and revoke certificates, OpenLDAP to store certificates and certificate revocation lists, OCSPD is an online tool to verify the status of the certificates, Apache, EJBCA the Open Source certification authority that have implemented the most used cryptographic protocols, all the software packages mentioned above are important and have a relevant role in construction of the proposed ROPKI architecture.

Usually a BCA does not issue certificates straight to users, nor is the confidences that the hierarchical architecture, BCA carrying out point-to-point links with PKI infrastructure and lets users keep the points of initial trust. These links are combined to let users to interact with members of different communities by means of BCA's, in a secure way. If the BCA site interacts with a hierarchical PKI infrastructure is realized in a relationship of trust with the root CA, if the BCA site interact with a mesh PKI infrastructure is required to make reliable bidirectional connection with one of CA elements of the newer sites.

The proposed architecture exemplified in Figure 1 is the architecture intended for the national ROPKI system. Comprises of RO-BCA that will be established and other public key infrastructure from public administration, in this picture is presented a governmental agency (CA-A) authority from public sector and another authority from private provider (CA-P), at this time in Romania are three private providers who have their own CA used to issue and sell qualified certificates to Romanian citizens. In addition, it's interdependence with European Bridge Certification Authority (EGCA) to link with other existent certification authorities from Europe which is already joined to EGCA.

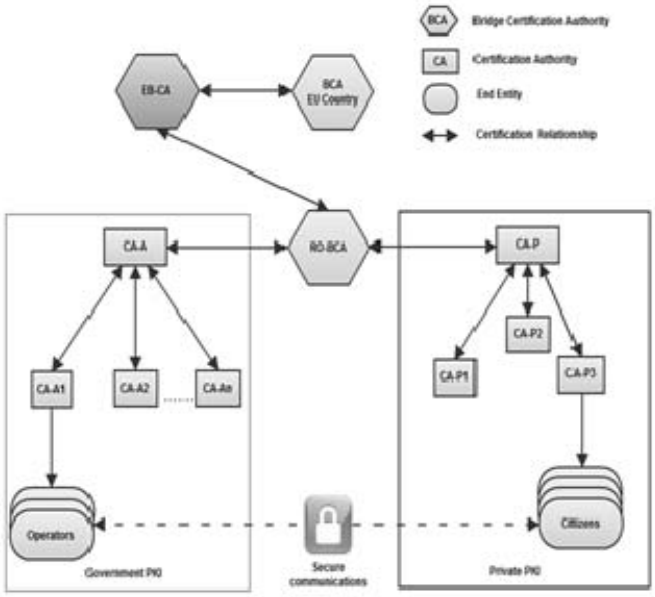

Figure 1. RO-PKI proposed architecture.

The digital certificate validation is realized through validating certification path between two or more CA, for instance if an Operator wants to communicate with a Citizen, he must verify certificates from this certification path as in (1):

Citizens -> CA-P3 -> CA-P -> RO-BCA -> CA-A (1)

In addition, for citizens we have (2):

Operators -> CA-A1 -> CA-A -> RO-BCA -> CA-P (2)

Users will use the relationship of trust made in the BCA's between those two points of trust (CA-A and CA-P) in order to interact safely.

6. Conclusion

Millions of citizens use PKI every day, the majority without being aware that they have been using it. PKI is already proven that provides to any user with a need to secure email, a secure channel to make payments over the Internet. However, PKI has succeeded by assuring his security services it has failed against its detected potential. A nationwide public key infrastructure is a crucial point in the evolution of public administration services and to provide citizens the possibility to perform secure electronic transactions with the public institutions. PKI performs a significant role in the countries that already have embraced this solution because it offers three relevant services, namely: authentication, digital signature and encryption and all of these are possible ensuing issuance of a qualified digital certificate, trust established for these types of certificates help agencies within the public administration to offer more competent services to citizens, reducing the risk of forgery or loss and spreading information in an easy and secure manner.

Reference

[1] Larry Caffrey, Rogers W'O. Okot-Uma,"Trusted services and public key infrastructure (PKI)" , Commonwealth Secretariat, 2001.
[2] Nicu□or Vatră, "Public key infrastructure overview", Scientific Studies and Research, Series Mathematics and Informatics, no. 2, vol. 19, 2009, pp.471 - 478.
[3] Carlisle. Adams, Steve Lloyd,"Understanding PKI: Concepts, Standards and Deployment Considerations", Addison-Wesley Professional, 2 edition, 2002.
[4] Andrew Nash, "PKI: implementing and managing E-security ", Osborne/McGraw-Hill, 2001.
[5] Denis Trček ,"Managing information systems security and privacy", Birkhäuser, 2006.
[6] Klaus Schmeh, "Cryptography and public key infrastructure on the Internet ",John Wiley and Sons, 2003.
[7] Suranjan Choudhury, Kartik Bhatnagar, Wasim Haque, "Public key infrastructure: implementation and design" , John Wiley & Sons, 2002.