Simulation and design of the Public Key infrastructure based on X.509 digital certificates through free software so that they are used in email security at the Cuerpo de Ingenieros del Ejercito - Quito headquarters office internal data network

Carlos A. Vásquez, David R. Valencia

***Abstract*— This document contains information related to the Infrastructure 's design of the Public Key that issues X.509 digital certificates used in the information security that its transferred via institutional email at the Cuerpo de Ingenieros del Ejercito de Quito.**

This solution totally developed under free-software tools, provides a security system that complements the protection level guaranteed by the actual systems at this entity. Improved security mechanisms will be available and its application will be focused on the institutional email's protection. Eventually this protection will be used to protect and secure generated information by diverse applications and network services. Trying of implement in-depth security systems based on defense levels, a high security standard can be reached.

Index Terms*— *Public Key Infraestructure; digital certificate; certificate authority; register authority; certificate revocation list; public key; private key; encryption; mail transfer agent; mail delivery agent; mail user agent.

I. INTRODUCTION

The progressive technological development experienced has generated diverse telematics communication tendencies that have notably improved a person's living conditions. However, felony technical tendencies have evolved using communication networks that intend to "steal" or manipulate information thus producing loses and damages.

That is the reason why this we should pay attention to this research paper so the identity of users who are involved in telematics communications is proven as genuine and the conveyed information is manipulated only by legitimate recipients; considering that since remote times, the protection of information is fundamental, this fact, has definitely transcended until present time.

Document received on December, 2014. This research has been made as a previous project to get the degree in the Electronics and Communication Network Engineering of the, Faculty of Applied Science (FICA), of the "Universidad Técnica del Norte".

C.A. Vásquez, Works at the "Universidad Técnica del Norte", 17 de Julio Avenue, "El Olivo" neighborhood, Ibarra-Ecuador.

D.R. Valencia, graduate of the Electronics and Communication Network Engineering Career.

Throughout the Public Key infrastructure, it is possible to create a network service that issues digital certificates and manages user's activities. By doing so, an institutional secure email platform will be set up guaranteeing confidentiality, integrity, authentication on each message sent through this applying those certificates and cryptographic encryption techniques and digital signing.

II. BASIC COCEPTS

A. *Digital Signature*

It is a binary sequence that travels throughout the network and attaches a data message or document that guarantees its integrity and verification of the identity of the transmitter where it comes from providing a security mechanism within communication systems.

Technically is the combination of two security mechanisms, asymmetric encryption and hash functions. It would take a lot of computational resources to apply these functions about full documents. There must be a more efficient way to perform these functions. [1]

Criptography

It is the science that deals with encryption techniques that allow hiding information in order to preserve its confidentiality. Such techniques modify data messaging using a encryption algorithm and a key or key to interpret only those users bearing appropriate key.

By the use of cryptography, certain security services can be guaranteed such as confidentiality (turned into illegible data), integrity (using hash functions the remittent identifies whether messages have been modified) and non-repudiation (is a way to authenticate the message's origin). [1]

Hash Functions

Hash functions are used to create a document's digital print (signature), compressing it turns into an unfalsifiable bits sequence. In contrast, the usual sequences as ZIP, these should be irreversible with the purpose of safeguarding the document's integrity.

In order to generate a summation, several operations are done, depending on which algorithm is used (MD5; SHA1, among others). There are two kinds of hash functions: first operate directly over the content of data messaging at transmission time, they are called MDC (Modification

Detection Codes). Second uses a complementary key to authenticate users or devices before any system or network denominated MAC (Message-Authentication-Code). [2]

Key Cryptographic Distribution and Administration

The cryptosystems strength lies on the cryptographic keys privacy, so their administration and distribution depends on protocols and techniques of cypher that guarantee communication with remote reliable entities.

Within private key cryptosystems, generating keys is simple, but its distribution through insecure channels, involve complex protection methods. Asymmetric cryptosystems notably solved symmetric keys diffusion problems by the use of a key pair, private (secret) and public (openly shared) so databases, or public access directories know it and a user's identity is linked to this key.

The disadvantage is that the public key only contains a bit sequence that can be self-generated by anyone using computer means. Because of it, vulnerability exists and a method called Digital Certificate has been developed. This certificate is issued by any impartial entity (certificate authority) it links a person's identity with its public key. [1][2]

B. Public Key Infraestructure

PKI is a security system comprised by hardware, software, people and policies that secure the emission and digital certificates management based on cryptographic keys, endorsing user—public key relation to implant encryption and digital signatures mechanisms over a diverse set of telematics applications.

Functioning of PKI depends primarily on certification entities supported by the registry and directories authorities, they operate under certain control procedures established by security policies that manage digital certificates and focus on sensible information protection. [3]

Certification Authority(CA)

It is an impartial entity in which mutual trust exists between transmitter and receptor. This certificate acts as an intermediary that endorses communication among legitimate entities. It is in charge of verifying user or device identities issuing digital certificates linking them with a public key. Certificates publishing on public directories, renewal and revocation, in case keys have expired, change data registered, or key compromised.

Figure 1 shows a CAs ranked architecture which the root authority generates its own certificate endorsed by its digital signature (it certifies itself) thus supporting local environment users from a city or country. CA transmits digital signed certificates to intermediate authorities enabling subordinate authorities the certifying of end-users and end-devices after going through a verification and record registry. [4][5]

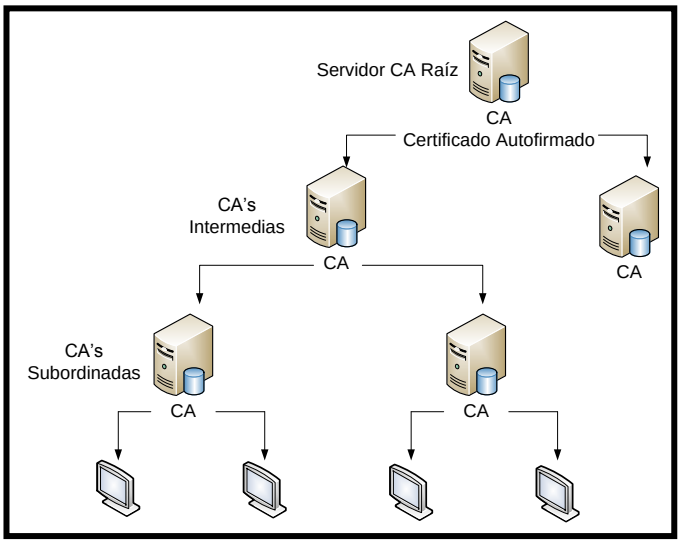

Fig. 1. Hierarchical architecture certification

Registry Authority(RA)

CAs perform diverse functions to certify intermediate or final authorities, but when PKI covers high demand user environments or geographically distant, efficient attention gets complicated as even CA may collapse by an activity overload.

Because of this fact, occasionally entities delegate processing management and authentication to a registry authority who requests verification. The advantage of using this additional authority is the scalability of the service so that most certification petitions get through end-users and end-devices previously authorized by RA.

It is the link between end user and CA that responds to record requests, certification and key retrieval; association between public key and certificate bearer, certificate life cycle management, focusing on reversal, expiration, renewal and reissuing of cryptographic keys and updated information certificates. [4][5]

Digital Certificate

It is a document that associates someone's identity to a computer device using a public key to show its reliability, avoiding potential spoofing over telematics applications of confidential nature. To probe possessiveness of an entity, person or computer device that contain personal data, public key, digital signature and other pertinent information, the UIT – T.X.509 standard that specifies data formats has been developed.

Digital certificates make possible interaction over diverse telematics applications such as secure web server access, intranets or virtual private networks, secure emailing etc. Their transmission varies depending on device type, addressee or sender. Fig 2 shows possible scenarios.

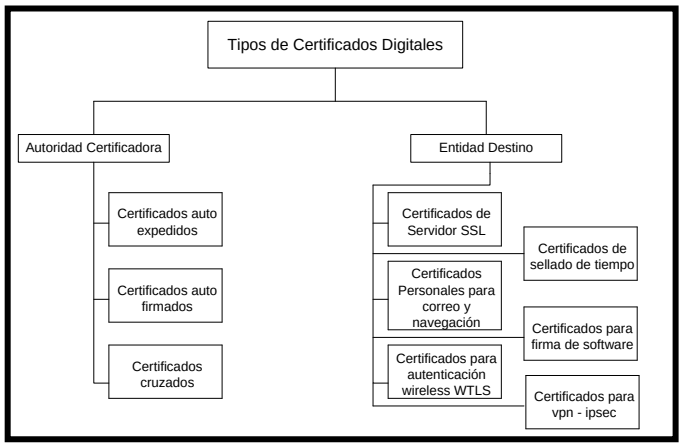

Fig. 2. Types of Digital Certificates

Certificates directory publication

These are services performed in PKI environments for certificates storing issued by CAs, keeping them available for user access and need to retrieve data to set up secure communication. It contributes to manage its distribution and expiration date by revocation lists. [4]

Certificate Revocation Lists (CRL)

Digital certificates are issued to lasts for a period of time, but there are several causes that may invalidate them without expiring them. If a user's private key is compromised or data is not updated for any reason. So the need for publishing a list by CA is to scan those certificates that for some reason have been invalidated. Any entity carrying a CRL directory is capable of checking certificates expiration dates.

This list has great importance regarding telematics applications because none of them will authenticate a person or device, will not accept a digital signature in which a certificate has expired. It is probable that a revoked certificate continues being used. [4]

C. E-mail

It is a service that allows transmission and reception of messages over communication networks by using computer systems set up as mailing services enabling the independent exchange of intermediary networks.

Components and functioning

They are structured according to the client's model. The server, which communicates through protocols that starts and ends on the other side of the client as messages are sent using a client's application called MUA (Mail-User-Agent) like Microsoft, Outlook, Eudora , Mozilla and Thunderbird.

Email servers are set up to perform two different transfer agent procedures (MTA-Mail-Transport-Agent). This agent forwards messages that the addressee manages and (MDA-Mail Delivery-Agent) stores messages in the corresponding mailboxes for post-delivery.

MUA identifies its server's outgoing configuration (MTA) to send a message. It gets transferred using a SMTP protocol (Simple Mail Transfer Protocol). The outgoing MTA uses the remittent address and initiates communication with DNS (Domain Name System) which is linked to, identifying the MTA's management domain. Then a TCP connection is set up with port 25 towards the MTA server transferring the original message. Finally this destination server verifies whether the receptor's address is in place and serves as MDA agent storing the message in the addressee's destination to its next download or visualization. Fig 3 shows this process.

E-mail Seurity

An alternative measure security is to protect the transferring of emails using secure emissions protocols like TLS. In order to guarantee reliability from one end to the other, it will be necessary to secure set up links between MTAs intermediaries. The only problem is that this network is designed to operate under storage—forwarding scheme, thus TLS protects in-transit data through the network as intermediaries or final (MDAs) become vulnerable. This fault can be avoided.

Therefore, security techniques have been developed to protect the transferring process to the addressee, without the implementation of complex security mechanisms over a transport or network layer, or even without modifying the email's infrastructure.

At present, most secure email platforms use cryptographic techniques in the MUA agents that generate self-protected emails over a encryption or digital signature on the application layer. By doing so, the MTAs will deliver emails to their proper destinations in a conventional way.

Some of the most commonly used security systems are PGP and S/MIME. PGP is based on the cryptographic par keys management (public and private). S/MIME is based on digital certificates; the only existing disadvantage is that they are not compatible. [6]

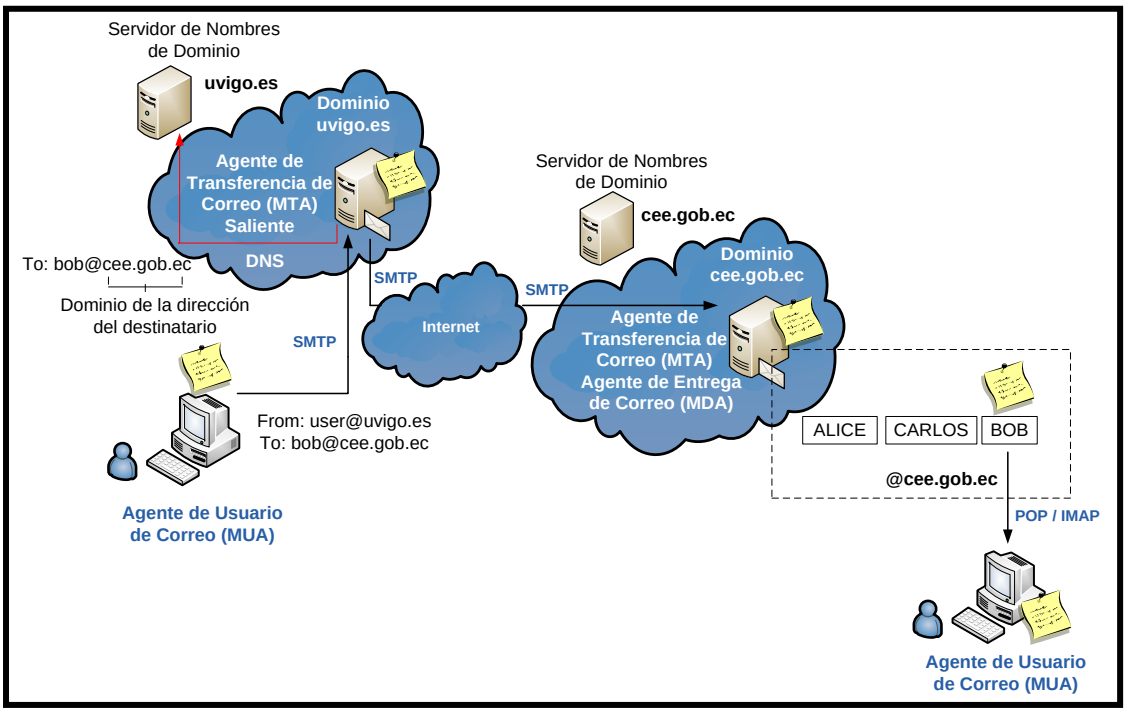

Fig. 3. Sending and reception of an email process

III. PKI AND EMAIL PLATAFORM DESIGNS INFRAESTRUCTURE

A. *Design's Criteria*

This project's main purpose is the Cuerpo de Ingenieros de Quito military's officials' certification performed through the issuance of digital certificates which legitimately link their identities to their public private key, evidencing the reliability of these entities.

The main objective is to set up a Headquarters Certifying Authority that becomes a legitimately authorized entity that self-generates certification procedures within the CEE's parameters. However, this entity not only issues certificates, it must also manage them by integrating additional components for the implementation of a Public Key Infrastructure. Table 1 shows these components.

TABLA I
ESTREUCTURAL COMPONENTS

COMPONENT	DESCRIPTION
Registry Authority (RA)	Responds to registration requests, keys /certificates retrieval, certificates life cycle management, use information updates among others.
Certificates Publication Directory	It will store certificates issued by users to obtain and use email security and protection.
Certificate Revocation List	It is a document that will permanently publish the CA, to let everyone know certificates that have been revoked (invalidated).

The functionality aspects when designing a PKI is linked to the type of certificates delivery since CA can be set up to be delivered via hardware and software means.

USB cryptographic tokens are hardware devices commonly used for digital certificates and private keys secure storing. As for software tools, the most common is the use of p12 o pfx format so that they can be stored in the final user's computer.

As a consequence, in the CEE PKI environment, user's certificates will be distributed using the p12 format. Eventually as the officials and authorities belonging to this entity are familiarized with the system, a token-usb distribution may be implemented.

The second part of this project is the design of an email platform based on free software tools that enable functionalities developed over Exchange, so that the migration of new systems provide similar services to private users investing much less or with no cost in their implementation.

The best alternative to protect this service is the use of the TLS protocol layer, but in order to guarantee a secure end-to-end communication, it would be optimal to cypher all intermediate links that could interfere during the transferring of data.

The ideal solution is to generate self-protected emails through encryption or digital signing within the application layer thus the MTAs transfer emails to their destination normally. Then protection during the entire transferring process is guaranteed, even if emails are stored in the receiver's mailbox.

As Institutional CEE e-mailing is being designed, this security method will be implemented using TLS protocols securing client / server communication links. The main protection mechanism will be the implementation of S/MIME to generate self-protected email.

B. *Operating Mode*

As a precautionary measure, the CEE official military end user must not be part of the certificate application process

within the institution's environment. They should only be trained and destined to utilize this security mechanism. As for the information being transferred via institutional email, only the network administrator will be able to carry out such activities.

Based on the previous statement, then the network's administrator must carry out such certification process as shown in Fig 4. Note interaction between PKI components and CEE.

Each institution's user has an installed legitimate certificate in their PC. At the same time, the MUA (emailing agent) will be set up over each user to integrate this certificate so that the S/MIME techniques will be activated protecting emails transferred with encryption and digital signing mechanisms.

At this point, user's PCs interaction regarding the sending of a digitally signed email is shown in Fig. 5.

1. Outlook's email transmitter generates a message throughout the S/MIME structure which will be signed using its private cryptographic signature.
2. This self-protected message will be transfer in a usual way over the SMTP transport protocol, TLS will be used to cypher communication channel, finally storing the message in the user's server.
3. The receiver will access his mailbox and download pending messages using POP3 protocol, with SSL to encrypt the connection.
4. S/MIME message obtained.
5. MUA agent will detect its structure and will get a X.509 digital certificate from the transmitter containing a validation message using CRL certificates revocation lists which PKI and CEE will publish constantly. Expiration date is validated and finally the digital signature is generated by the CA.
6. If the certificate is legitimate, digital signature message will be verified to assess if alterations have been performed illicitly so the transmitter' authentication is confirmed. The receiver must add the transmitter to his Outlook contacts , storing along with it its digital certificate that later will be used avoiding encryption messaging and guaranteeing that he is the only person who is able to see the message.

The same transferring process occurs in cases of encryption messages differing cryptographic operations. Fig 6 shows verification process.

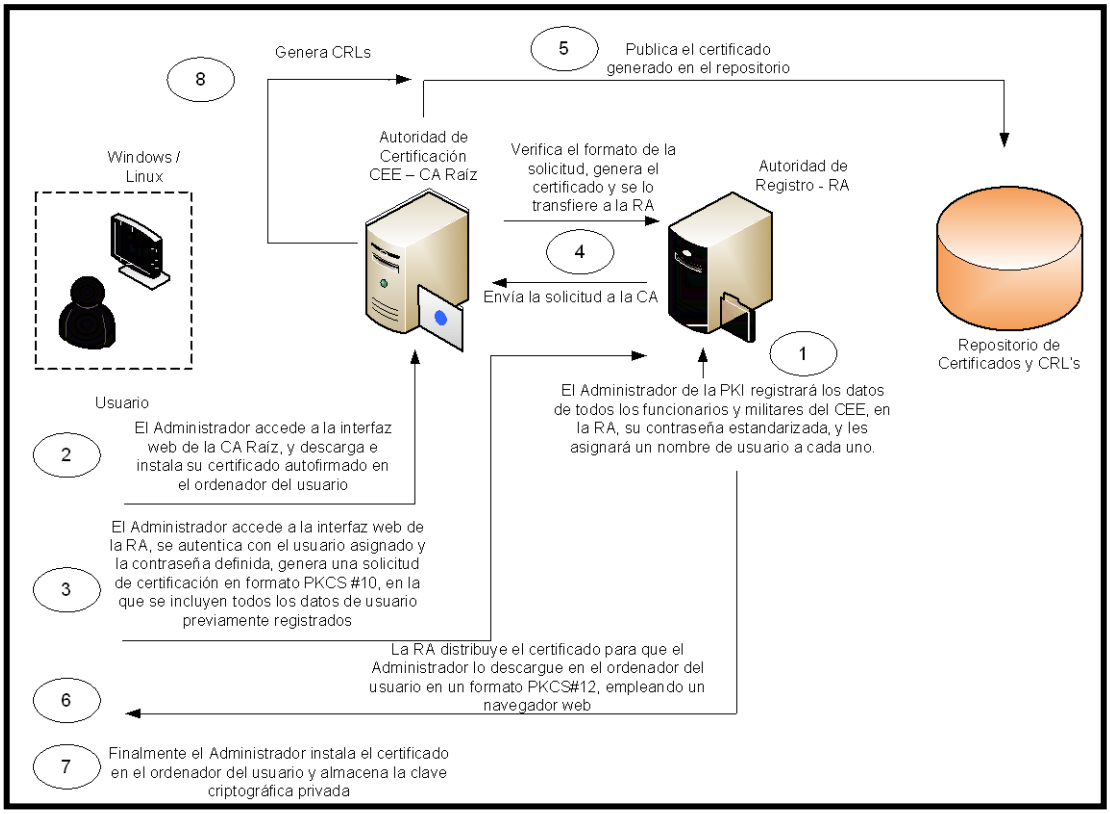

Fig. 4. Certification process within PKI environment

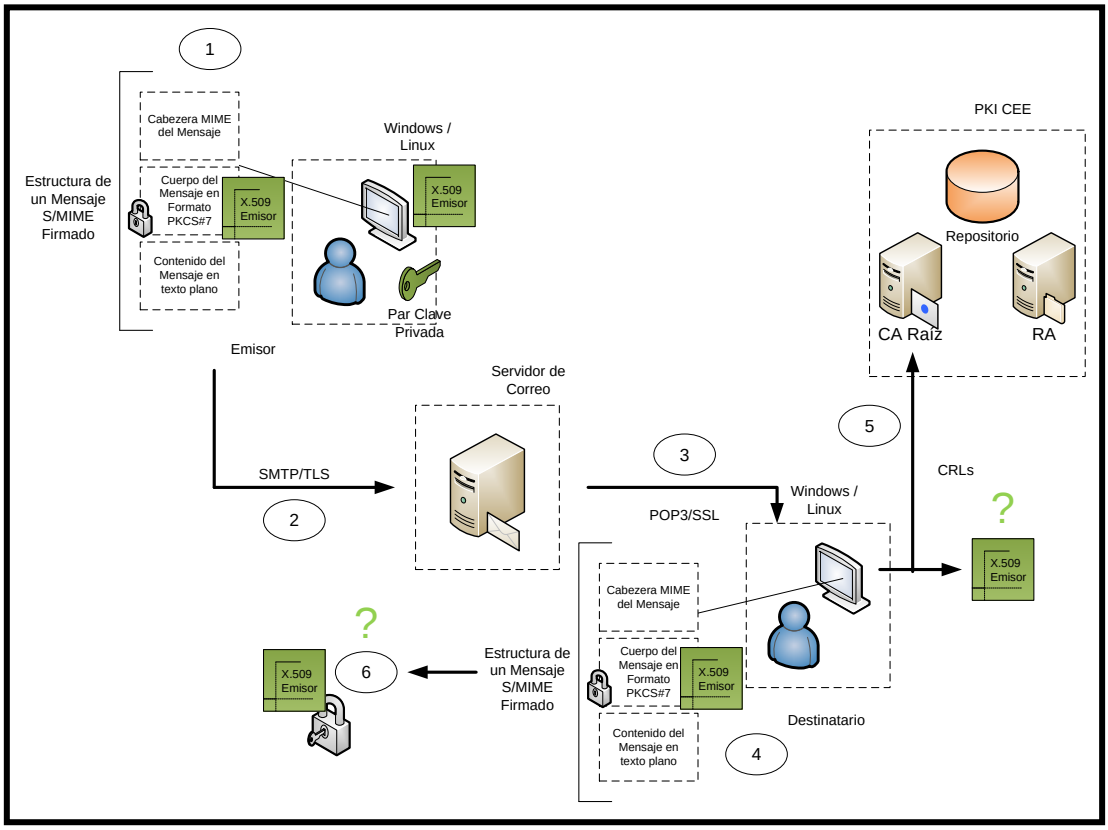

Fig. 5. User interaction, PKI and CEE email signature system

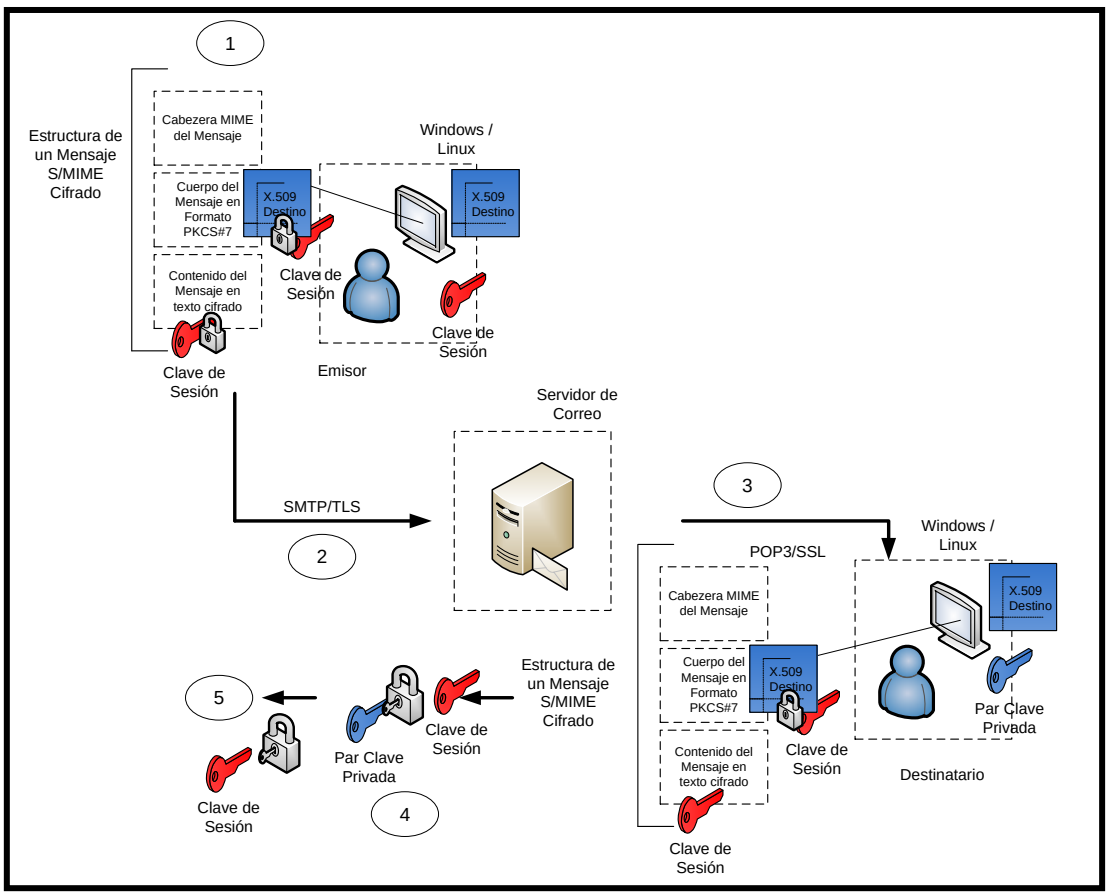

Fig. 6. User's interaction, PKI and email system within CEE environment—Encryption message

- The transmitter's computer generates a key session that will be encryption utilizing the receiver's certificate, guaranteeing that he is the only one who may decipher it using his private key. The contents of this message will be ciphered with the session's key.
- Addressee deciphers his session key using his par key, finalizing the process to revel message contents.

One of the most important requirements of this project is the mail box migration of information created by the current mail server (messaging, contacts, and calendar) developing Microsoft Exchange leading to a free software platform guarantee protected user information.

C. *Main used tools empleadas*

- **EJBCA.-** Is software that allows the implementation of a PKI, built on a J2EE base (Java 2 Platform, Enterprise Edition) able to perform CAs (Certification Authority and Records emission pertaining to CRLs) functions without using additional tools because this authority has been structured by components that comply with their assigned functions. [7]

- **JBOSS AS.-** Is an application server designed to hold the unfolding of high-performance business apps over J2EE. When this software is downloaded it operates under an open key license that makes downloading, installation, execution and free distribution without restrictions making this platform one of the most used in real production applications. Additionally it manages logistics over developed applications and when it comes to accessing data, this app does not need to programmed, it only takes assembling from the server modules.

- **ZIMBRA COLLABORATION SUITE (ZCS).-** Is a collaboration project that has developed a complete messaging open key offering a reliable high-performance emailing service featuring address books, agendas and additional tasks. It has been developed on JAVA basis, using Jetty as its application server; integrated by several Postfix based MTA systems, storing date for user information over the Open LDAP and MySQL base. It features a Cypher protocol SSL/TLS that incorporates security mechanisms like antivirus, antispam and a powerful Lucene search engine.

- **MICROSOFT EXCHANGE 2010.-** This is the software in which the emailing system has been displayed at the actual CEE –Quito.

D. *Hardware sizing*

Generally, relevant hardware parameters that must be considered before implementing a server are as follows: processor, RAM memory and storage capacity. To evaluate these parameters in this research, the following applications were contemplated: EJBCA, JBoss, MySQL, Zimbra, Collaboration Suite and the host operating system to guarantee proper operating.

Process capacity is determined by the behavioral analysis of a common user and involves knowing the executed operations time and how frequently these actions are done. Table II summarizes recommended hardware characteristics for the implementation of the preceding network services.

TABLA II
HARDWARE FEATURES

FEATURE	MINIMUM REQUIREMENT
PUBLIC KEY INFRAESTRUCTURE	
RAM Memory	4 GB
Processor (CPU)	2 cores operating at 3 Ghz
Hard Disk	160 GB
MAIL SERVER	
Memoria RAM	4 GB
Procesador (CPU)	2 cores operating at 3 Ghz
Disco Duro	160 GB

IV. PERFOMANCE TESTING

This testing implicates that each user has a digital certificate installed set up in Outlook to implement S/MIME protection techniques.

A. *Testing Scenarios*

The packages that try to infringe transferred messages confidentiality can be caught. Fig 7 shows the mail I question.

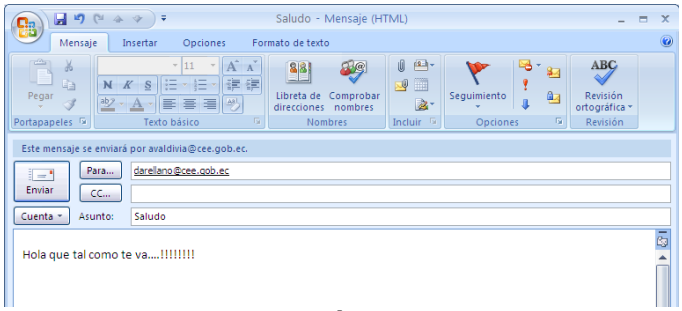

Fig. 7. Mail in question

This action was performed using the traffic's analyzer Wireshark over some types of messages.

Flat text message

Over the analyzer a filter is applied to capture a SMTP protocol. As the capture is initiated, right click and select option Follow TCP steam. This process allows visualizing a conversation as it occurred. Fig 8 shows results.

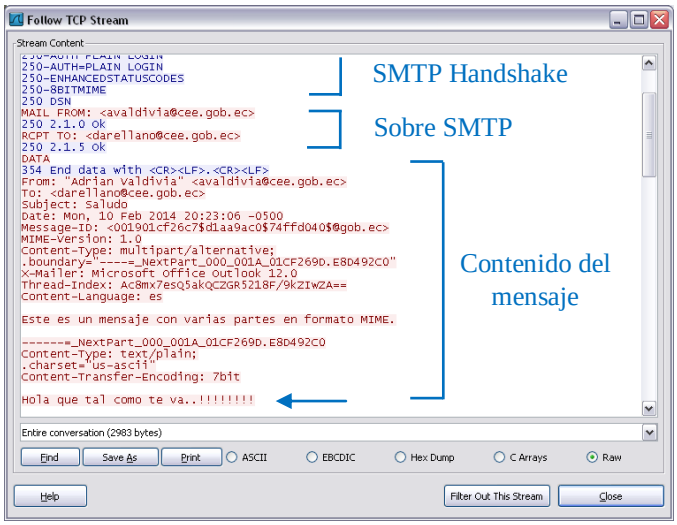

Fig. 8. SMTP Capture with Wireshark

Transmitter / receiver email addresses are revealed and the message itself can be visualized. This proves that messages do not oppose to any infringing techniques.

Encryption Message

The same procedure was applied and results are shown in Fig. 9.

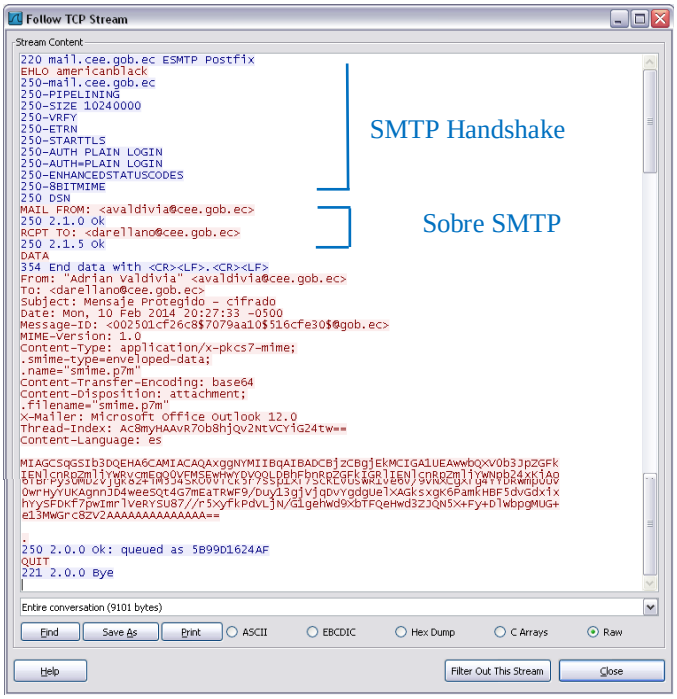

Fig. 9. SMTP Capture with Wireshark

Notice that the first two structural massage fields have not varied. However the message body has turned into a legible format thus generating self-protected transferred messages being stored appropriately.

Encryption transferred message using TLS

The same process is used while the client's Outlook email is activated. This protection protocol is used over the transport layer. Fig 10 shows results.

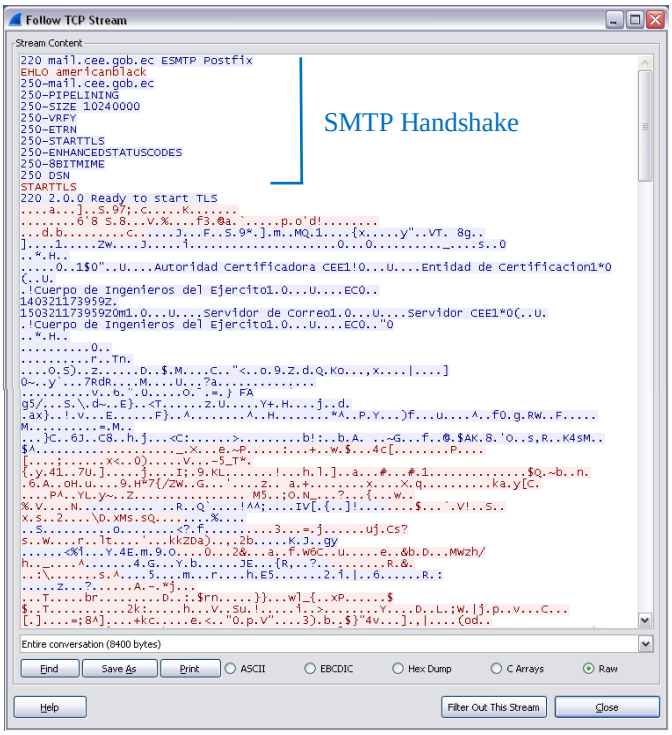

Fig. 10. SMTP Capture with Wireshark

This mechanism complements the security system, hiding over the SMTP that contains origin/destination email addresses. This result is useful when hackers do not care about revealing message contents, but to find out whom it is from and to whom the message is directed. This option would allow them to manipulate specific information.

The above it is safely concluded that the utilized tools and configurations realized in this project comply with email security institutional regulations.

V. Conclusion

Reliable email message transferring is guaranteed through the implementation of cryptographic mechanisms that protect them while they are in transit over the networks based on TLS protocol. An effective protective alternative capable of protecting emailed messages at mail box storage stage are S/MIME extensions; securing communication from one end to another. These extensions operate over each application layer, generating self-protected messages allowing the performance of a digital signing implementation mechanism.

During Public Key Infrastructure design, it's essential to point out the strategic location of the CA Root, separating it from the servers CEE homestead to preserve the certification systems operating mode. The objective is to restrict access to this server protecting its cryptographic private key.

Certification hierarchy set up by the Cuerpo de Ingenieros del Ejército—Quito is based on a flat architecture being CA Root that directly certifies end users, having the option of complementing the process using CA subordinates or intermediary to broaden certification services performed from remote locations.

EJBCA Front-end administration works according to a number of certificates issued, so when users try to infringe a digital certificate, they will have to go through PKI using PKI's resources. This can only take place after a certificate may be authorized.

Public Key Infrastructure designed complied with the issuance purposes and X.509 digital certificates management.

Compatibility was reached with MUA email user agents in order to cypher and sign transferred messages digitally by this means.

This project has demonstrated that the integration of a security mechanism based on personal digital certificates is possible through newer communication platforms that may be applied to email messaging protecting the flow of information that goes around through these means.

It was proven that in fact, messages were protected during transferring process, being solely sent to legitimate end users; allowing them to revert encryption messages, to verify the integrity of a digital signature and to check sender's authenticity.

ACKNOWLEDGMENT

We express a special acknowledgment to the Department of Systems of the "Cuerpo de Ingenieros del Ejército de Quito", highlighting to Ing. Freddy Chuquimarca, Network Administrator of this institution, and Captain Braulio Moreno, by openness, support and collaboration provided to development of this project.

REFERENCES

[1] Stallings, W. (2006). Cryptography and Network Security Principles and Practice. Recuperado de http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/.

[2] Lucena, M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de http://es.scribd.com/doc/39400098/Criptografia.

[3] Cuesta, J., & Puñales, M. (2002). Seguridad en Redes Telemáticas-Infraestructura de Clave Pública (PKI). Recuperado de http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI.

[4] INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

[5] Osorio, J. M. (s.f.). Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

[6] Perramon, X. (s.f.). Aplicaciones Seguras. Recuperado de http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf

[7] Ayesha, I. G. & Asra, P. (2006). PKI Administration using EJBCA and OpenCA. Recuperado de http://teal.gmu.edu/courses/ECE646/project/reports_2006/IL-3-report.pdf.

Tutor – Ing. Carlos A. Vásquez A.

Born in Quito, province of Pichincha on September 19, 1981. Electronics and Telecomunications Engineer "Escuela Politécnica Nacional (EPN)", Quito-Ecuador, in 2008. Currently, teacher of the Electronics and Communication Network Engineer Career (UTN), Ibarra-Ecuador. He passed the CCNA 1, 2, 3 and 4 courses in the period June 2006 - March 2007 at the "Escuela Politécnica Nacional", and studying for a Master degree in Communication and Networks, "Pontificia Universidad Católica del Ecuador", Quito-Ecuador.

David R. Valencia T.

Born in Ibarra, Imbabura on May 30, 1987. Second son of Nelson Valencia and Gladys de la Torre. Primary education was made in the School "28 de Septiembre". He studied in the "Teodoro Gómez de la Toore" school, Ibarra-Ecuador. He studied Electronics and Communication Network Engineer at the "Universidad Técnica del Norte" , Ibarra-Ecuador.