Security Analysis of the Digital Fiscal Documents in the Mexican Tributary Administration System

Vladimir González-García
National Laboratory on Advanced Informatics
LANIA A.C., Xalapa, Veracruz México
vgonzalez@lania.edu.mx

Francisco Rodríguez-Henríquez
Computer Science Department
CINVESTAV-IPN, México City, México
francisco@cs.cinvestav.mx

Nareli Cruz-Cortés
Center for Computing Research (CIC)
National Polytechnic Institute (IPN), México
nareli@cic.ipn.mx

Abstract

Since January 2005, the Mexican Government, through the Tributary Administration System (SAT), offers the service of generating digital fiscal documents by using the so-called advanced electronic signatures. In this paper we point out several security flaws in the security protocol specified for generating those electronic invoices. Specifically, we show that the authentication process stipulated by SAT implies a critical security gap. We provide recommendations in order to avoid the security problems detected, which includes the usage of alternative authentication protocols, Time Stamps Authorities and Digital Notary.

1 Introduction

During the last twenty years we have witnessed how the information technologies, such as Internet, have changed our daily life. Nowadays, Internet is used for transmitting voice, video and tv programs, publishing newspapers, performing electronic commercial transactions, etc. One innovative application that makes use of the information technology tool is the so-called *e-government*.

e-Government can be informally defined as the government's use of information technologies to exchange information and services with citizens, enterprises and other branches of government. The main goal of the e-government is to improve the internal efficiency, as well as the prompt delivery of public services and/or processes of democratic governance.

Several countries in Latin-America have established the necessary laws to regulate the governamental/commercial transactions through the Internet. For instance, Puerto Rico established its own normative since 1998. That step was followed by Colombia in 1999, México and Perú in 2000, and Argentina and Venezuela in 2001.

In the specific case of México, since January 2005 the Mexican government, through the Tributary Administration System (*Sistema de Administración Tributaria de México*, SAT), has offered to taxpayers a system for the automatic generation of electronic invoices (*factura digital*) or *Comprobante Fiscal Digital* (CFD). The CFD service is intended for the automatization of the accounting process of individuals and enterprises, by allowing to all taxpayers, Internet access to fiscal and administrative services. Up to this date, the utilization of CFDs is not mandatory, however, its use will be declared compulsory by SAT´s in a near future [4].

Since 2005, the CFD service has gradually gained a greater importance, among other reasons, because of the increasing number of Mexican enterprises that have the aim of achieving and automatic accounting process. For example, in the case of the Mexican federal government only, the list of its branches and decentralized dependencies that already utilize electronic invoices for tax and administrative declarations include: *Banco de México, Secretaría de la Función Pública, Secretaría de Economía, Instituto Mexicano del Seguro Social*. Moreover, from January 5th, 2005 to March 16th, 2007 a total of 1909 taxpayers had used the CFD service, 254 of them are regular taxpayers ("*Personas Físicas*") and 1657 are company representatives ("*Personas Morales*"). Furthermore, 4,136,707 CFDs have been issued so far by the Mexican government [4].

It should be noticed that the SAT's CFD service implies the exchange of confidential information over communication channels that are intrinsically highly vulnerable. There-

fore, it becomes indispensable to incorporate to this service reliable and sound information security mechanisms. In the case of CFDs, their security lies on *digital signatures*.

The concept of digital signature is analog to the real-world autograph signature, but it is more powerful in the sense that it also offers protection against malicious data modifications. In this way, the Digital Signature provides juridical and technical protection to electronic documents, as well as commercial transactions.

Unfortunately, digital signatures by themselves cannot provide reasonable protection against several sophisticated authentication attacks such as man-in-the-middle attack, identity-misbinding attack, identity usurpation, and so on [15]. Other potential devastating problems include the lack of protection against senders/receivers that refuse to acknowledge that they have send/receive a given document.

Because of that, CFDs incorporate the usage of an infrastructure able to overcome aforementioned security gaps. That infrastructure is known as Public Key Infrastructure (PKI) [10], and in the case of the SAT's CFD service it has been implemented according to the PKCS Standards [4].

In this paper, we carefully analyze the security protocols associated to the SAT's Electronic invoice service. We list a number of security flaws that can be found in the SAT specifications. Furthermore, in order to fix/improve those security weaknesses, we recommend several modifications to the current SAT protocols. In particular, we strongly recommend the specification of a secure storage of all the CFD created by an enterprise and/or individual. Apparently, this measure has not been considered at all in the official SAT´s procedure.

The rest of this paper is organized as follows. In § 2 we briefly summarize the most important security information concepts and services used throughout the manuscript. Then in § 3 we outline the main procedures that specifies the SAT's advanced digital signature FIEL protocol. In §4 we point out several security flaws in the FIEL protocol, whereas in §5 we give security solutions to the problems detected. Finally, in §6, some conclusions are drawn.

2 Basic Security Notions

In 1976 Diffie and Hellman introduced the concept of public key cryptography. Public key crypto-schemes are characterized by the fact that a pair of public and private keys is assigned at each user in the system, with the property that if a public key is used for encrypting (decrypting) messages, then only the corresponding private key can be used to decrypt (encrypt) them, as is shown in Fig. 1.

In modern cryptography, however, public key crypto-schemes are mainly used for generating digital signatures, which theoretically cannot be forged. In general, a digital signature should exhibit the following three properties,

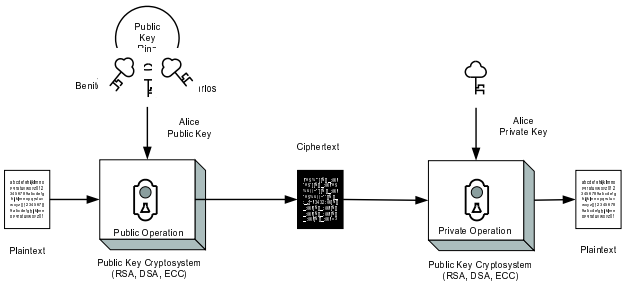

Figure 1. Public Key Encryption/Decryption

- Integrity: It implies that the received document is a genuine identical copy of the one that was sent.
- Identity: It ensures that the received document was created by a determined author.
- Non-repudiation: Neither the sender nor the receiver, can deny having sent or having received a document.

Fig. 2 shows the typical process followed in order to sign/verify a digital document.

However, as it was mentioned in the preceding section, public key cryptography alone, cannot provide reasonable protection against several authentication attacks. Concretely, the sort of security concerns posed by the application of public key algorithms without the support provided by an additional infrastructure can be classified into the following four types [15]:

1. *Secure Key Authentication*. It is crucial to avoid attacks like man-in-the-middle and identity usurpation attacks.
2. *Key revocation*. In the case that A's private key has been compromised by the opponent, then A has no option but to generate a new pair of keys while his/her old ones must not be used anymore (an action known as *key revocation*). However, it remains as an open problem how to announce to all A's correspondents that A's keys have just been revoked.
3. *Non-repudiation*. The main goal of a digital signature is to offer the *non-repudiation* security service, under the assumption that if A keeps his/her private key in secret, then nobody else can generate a digital signature but himself/herself. However, A could deny his/her alleged digital signature by arguing that the signature does not correspond to his/her secret key.
4. *Policy application*. The only concerted way to enforce security policies among a large community of users is by mean of an external infrastructure of authority entities.

Consequently, it is customary to complement the usage of public key Cryptography using the so-called Public Key Infrastructure (PKI) [10]. The *de facto*X.509 PKI [5, 7] and PKCS [9] standards comprise a collection of software, cryptographic technologies and services that allow the protection of the information transactions security in a distributed system. This way, PKI X.509 and PKCS standards integrate *digital certificates, public key cryptography and Certification Authorities (CA)* in a single security architecture. In particular, PKI X.509 defines a digital certificate as a document that binds user's information (such as name, address, organization, etc.) to his/her corresponding public key. It is signed by a CA in order to guarantee its validity and integrity.

3 The Advanced Digital Signature Security (FIEL) and its protocol

The Advanced Electronic Signature [1] (FIEL after its name in Spanish), is the implementation of a digital signature based on the PKI standard specified in [9]. According to the Mexican Federal Fiscal Code published in [18], every taxpayer must require his/her FIEL. Up to this date, however, for some services the usage of the FIEL is optional [4].

In Mexico, an electronic invoice is a legal digital document with fiscal validity that follows the standards defined by SAT [16]. The security on a FIEL document is obtained when the sender signs a Digital invoice with his/her private key and the receiver verifies it using his/her public key according to the procedure outlined in Fig. 2. Furthermore, SAT established that all electronic invoices must be stored by users for a period of at least 5 years and destruction of them should be carried on only after 10 years of the issue date [4].

In the rest of this Section we will describe the security architecture utilized by the SAT for the FIEL and CFD generation.

3.1 The accounting must be electronic and simultaneous

In order to create a digital invoice, it is mandatory to use electronic connections such as Internet. Additionally, the user´s accounting register should be affected at the same time that the digital invoice is being generated. Furthermore, it must be guaranteed that the date, hour, minute and second in which the accounting register was affected is exactly the same that the one registered in the digital invoice.

[1] *Firma Electrónica Avanzada.*

3.2 Keys Generation and Certified Request

A 1024-bit RSA private/public key is generated in an electronic file of 1024 bits with name´s extension "*.key", as defined by the standard PKCS#8 [12] and ciphered according to the standard PKCS#1 [13]. The private/public key can be obtained through an application developed by the SAT which is available at the Internet called SOLCEDI (after its name in Spanish: *solicitud de certificados digitales*). SOLCEDI uses the open code library OPENSSL, however the key pair can be generated with any other library that complains with the aforementioned standards.

The FIEL certificate is an electronic document with name´s extension *.cer in the format X509 V3 [7] generated by the SAT. It binds user's information (such as name, address, organization, etc.) to his/her corresponding public key. In order to guarantee its validity and integrity, it is signed by SAT.

According to the procedure specified by SAT, a user FIEL certificate is granted in the SAT´s office only. The interested user should ask for an appointment and if the FIEL certificate is granted, the corresponding *.req file will be stored in a 3.5 inches magnetic disk (the only storage media allowed by SAT).

3.3 Folios

Taxpayers must request the approval of electronic folios by SAT, which are composed by a *series* and a number. In case of consent, SAT gives an approbation number. The system guarantees that the electronic series are different than their regular paper invoice counterparts. In order to guarantee that no folio is duplicated, it is necessary to verify that the folio number utilized in an electronic invoice corresponds to that of the approbation number given by SAT.

User's request for folios are accomplished by following two main steps. Firstly, it is necessary to request a folio´s certificate and second, the folio´s approbation range. The folio requirement procedure is performed through the SOLCEDI program that generates a file *.req and *.key under the PKCS standards. The *.req file is encapsulated with the FIEL certificate under the PKCS#7 [11] syntax by creating a file type *.sdg which should be send by Internet using the Digital Fiscal Documents System module (*Sistema de Comprobantes Fiscales Digitales*, SICOFI) available in [4]. Once the folio certificate has been obtained it is possible to request for folio approbations.

In order to keep and use his/her folio numbers, the taxpayer should prepare his/her administrative accounting systems to store folio numbers and series. Furthermore, it is necessary to validate the folios numbers to avoid duplications and numbers out of range in the taxpayer´s accounting

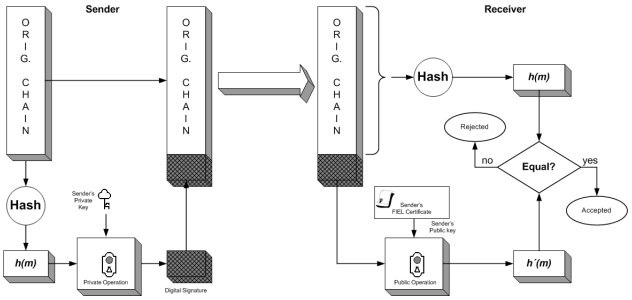

Figure 2. Digital Signature/Verification

system.

3.4 The Advanced Electronic Signature Generation

The Digital Signature is generated by following the next steps (which have been outlined in Fig. 2):

1. Original Chain Generation. It is a CFD´s that includes all the relevant data of the invoice as it has been defined and published in [16]. The original chain should be generated under the standard UTF-8.

2. Obtaining the Hash. It is an algorithm that generates a hash of the original chain, using the hash function MD5.

3. Signing the Hash. By using 1024-bit RSA as defined in the standard PKCS#1 [13], this signature process ensures that the digital invoice was signed by the legitimate owner of the private key. The resulting signature should be coded in format base 64.

After above three steps have been accomplished, a Digital Signature is obtained. In order to verify the Digital Signature, the sender´s public certificate should be downloaded using the program CERTISAT, then the signature verification is done with the certificate´s public key.

3.5 CFD Format

The generation, interpretation and storing of a CFD, as a digital invoice, must follow the format XML. The version 1 of this format was published in [16], and version 2 in [18], any of these two versions can be used. The format XML defined fields that contains fiscal data. Any additional information (such as commercial information, bar codes, number of purchase, discounts, special offers, time stamp, etc.) can be inserted into the invoice with a label called “addenda”.

3.6 Monthly report

Every month, it is necessary to report the folios that have been utilized. Currently, this report must be done through the SAT´s web page (SICOFI). The monthly report must contain the date, hour, minute and second in which the accounting registers and the electronic invoices were issued. The format for folio reports was specified in [16]. This report must be signed by the SAT through the module SICOFI.

3.7 Communication with SAT

At present date, it is necessary to have a direct connection to the SAT´s web page in order to validate folios, certificates and monthly reports. SAT was supposed to offer to taxpayers the necessary components for executing automatic validations through the Internet (i.e., web services). This service was projected to begin at 2005, however until now, still is not available.

3.8 Printing the Electronic Invoice

The SAT in [17] establishes that, in addition to the requirements published in [2], the electronic invoice must contain the original chain, the folio´s certificate serial number, the digital signature and the label: “Este documento es una impresión de un comprobante fiscal digital”. [2]

3.9 Storage

Every generated and/or received invoice must be stored in its original format XML. In [3] it is established that the taxpayer must store the XML file in their fiscal address during a period of at least 5 years. The receiver has the option to store the invoice as a copy of paper or as a file in the format XML. It is important to note that the storing should be into the fiscal address registered by the SAT, otherwise, if this were not the case, then it should be notified to the SAT.

The SAT does not consider secure storage of electronic invoices; as a result the user is left “on his own” for defining the necessary policies about this point.

3.10 Certificate Revocation

It is possible to revoke both, the FIEL certificate and the folio certificate. Certificate revocation can be accomplished by taxpayers through the Internet or by visiting the SATs offices with the corresponding documents and credentials [4].

[2] “This document is a digital fiscal invoice printed copy”.

To perform a certificate revocation by Internet, it is necessary to have the revocation key and the certificate. In order to know the current Certificate Revocation List (CRL) [7], it is necessary to access the SAT´s web page [4]. The SAT should implement a web services called on line Certificate Status Protocol (OCSP) as specified in [14], so that taxpayers can consult on-line which certificates have been revoked. Once again, this service was projected to appear at 2005, however, still is not available.

4 Problems

In this Section we briefly outline some of the most important security flaws that the SAT's electronic invoice system has.

4.1 Authentication Using the Private Key

In order to access SAT´s services, it is necessary to login by using either the CEIK (Confidential Electronic Identification Key) or the FIEL certificate. The CEIK authentication consists of giving to the system the taxpayer federal register key (RFC by its acronym in Spanish: "*Registro Federal del Contribuyente*") and a pre-agreed password.

In the case of the FIEL certificate authentication, the SAT´ system ask for the certificate, the private key and corresponding password. This is of course, unacceptable because the private key and the password should never be revealed by the user to anyone, *quite especially*, to the government. If the private key and the password are sent through the internet their security is compromised due to the possibility of the man-in-the-middle attack. Even if this attack is not launched by an anonymous opponent, SAT officers will have access to each one of the taxpayers' private keys and thus, they will have every means for generating electronic invoices on behalf of any taxpayer.

We strongly believe that this security leak in the SAT´s system must be corrected immediately, because it denies privacy to all the taxpayer community.

4.2 Date Manipulation

As it was stated in the previous Section, the generation of a Digital Invoice (DI) implies the simultaneous modification of the accounting register and the DI´s date and time. The DI and accounting register are controlled by the taxpayer´s software, then it is perfectly possible to change the actual date and time at any moment, even without the SAT´s knowledge. As a consequence, it could be possible to falsify documents if the client and provider agree on that.

4.3 Using the certificates

The PKI standards mandate that the Certificate Revocation List (CRL) should be publicly available and periodically updated. Otherwise, there exist an enormous number of ways for an attacker to launch attacks against the system as discussed in for example [20].

On the other hand having an on-line certificate revoking system might be useful in the case of the folio certificates. However, it might be a problem for the FIEL certificates due to the fact that a malicious intruder could easily revoke FIEL certificates invalidating the legally created ones. It could be even worse if the intruder knows the taxpayer private key and password, because he/she could renew the FIEL certificate using his/her own data.

A more mundane problem is that the first time that a taxpayer requires a FIEL certificate he/she must carry on the request file in a 3.5 inches magnetic disk to the SAT´s offices, which is a technology quite obsolete.

4.4 Cryptographic Algorithms

The FIEL and folio certificates are generated using cryptographic algorithms that are already obsolete or soon will be. The hash algorithm MD5 has been already broken. Moreover, it has been speculated that given the current technology and state-of-the-art factorization algorithms, 1024-bit RSA will not last more than 5 years. After that point, all standards will recommend to move on to 2048-bit RSA, in order to guarantee a reasonable security margin.

4.5 Unsafe storing

According to SAT, all electronic invoices generated by a user, should be kept into the fiscal address by a period of 5 years [3]. The format required to store those documents is XML. However, as it was mentioned above, the cryptographic algorithms used in the system will probably be compromised after a shorter period of time, and as a consequence, the CFDs stored in XML will become vulnerable. It is important to define a mechanism to safely store the information and renew the cryptographic algorithms in case that they get broken in the near future.

5 Recommendations

5.1 Taxpayer Authentication

The taxpayer authentication can be done without compromising the corresponding private key. A simple solution is outlined next:

- The taxpayer asks for a secure session to SAT, sending his/her digital certificate.

Table 1. Security Equivalence between Public Key Cryptography and Private Key Cryptography

	Security Level in Bits				
Cryptosystem	SHA-1 (80)	3DES (112)	AES (128)	AES (192)	AES (256)
ECC	160	224	256	384	512
RSA	1024	2048	3072	8192	15360

- SAT sends a session key encrypted with the user´s public key as a challenge to the taxpayer.
- The taxpayer decrypts the challenge with his/her private key.
- The taxpayer authenticates to the SAT´s web page using the session key.

Those steps would only require that the taxpayer uses a program to decrypt the challenge applying his/her private key.

5.2 Digital Fiscal Documents Generation

A Time-Stamp Authority verifies that the registered time and date have not been suffered any modification. The service given by this authority may be operated as a Trusted Third Party (TTP) [1]. The protocol Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) [1] defines a time-stamp authority, specifies the service requirement, the type of answer given, the errors, the security methods to be used, data structures and the certifier authority requirements. A time-stamps service is capable of processing verification requirements, that is, to verify that a data existed in a determined date and time. If a time-stamp server is used, it can be ensure that the date and time in the accounting register and the CFD have not been modified either maliciously or accidentally.

5.3 Alternative Cryptographic Algorithms

A sound alternative to RSA public key cryptosystem is Elliptic Curve Crypto-schemes (ECC). ECC has been carefully analyzed over the last 20 years and security experts believe that ECC can offer the same security than RSA using key lengths that are roughly ten times smaller. Having smaller keys is an important advantage in terms of performance and efficiency. Similarly there exist several new proposals for hash functions, other than MD5 or SHA-1, that have not been compromised yet.

In order to quantify the crucial importance of selecting the right cryptographic algorithm combination we give the following definitions.

We define the security strength of a strong n-bit key symmetric block cipher as the computational power needed for trying all possible keys, an attack traditionally known as *brute-force attack*.

We say that an m-bit key public key cryptographic algorithm has an equivalent n-bit security strength, with $m > n$, if the best known crypto attack to it, requires a computational effort comparable to the one associated to a brute force attack over an n-bit key strong symmetric block. Table 1 (which has been adapted from [6]), shows the security equivalence among two public key cryptosystems, namely, RSA (the one employed in the FIEL certificates) and ECC; against one hash algorithm, namely, SHA-1, and two symmetric ciphers, namely, 3DES and AES.

Mainly due to functionality or compatibility reasons, algorithms of different strengths and key sizes are frequently used together in the same application. In general, the weakest algorithm and key size used for cryptographic protection determines the strength of the overall protection provided to the system. As an example, if a powerful hash function with 128 bits of security strength is combined with 1024-bit RSA, then only 80-bit of security strength will be provided to the digital invoice. As it is shown in Table 1, should the application require 128 bits of security, a 3072-bit RSA key must be used. Likewise, 256-bit ECC can be used to substitute RSA as a public key cryptographic engine, providing the same security strength.

5.4 Safe Storage

If someone needs to certify a paper document, it is necessary to go to the notary to ensure its legality. The notary legalizes and saves one copy of the document with the goal of proving its authenticity. If a digital document requires certification then we can go to a Certificate Autority (CA) to verify and legalize the digital signature. However,

How can we legitimate that the CFD´s issued date and time are the original ones?

The answer to this question is to certificate the CFD with a Digital Notary which will have valid cryptographic algorithms into the next 10 years. Because of that, we propose the usage of cryptographic tools such as Digital Signatures and Time-Stamps in order to create a Notary Authority. This authority can certify digital documents, specifically Digital Invoices. For that end, it is possible to use a client-server architecture as the one shown in Figure 3. The Digital Notary may archive all digital invoices and digital certificates using Evidence Record Syntax (ERS) and the communication protocol LTAP [8] defined by the working group LTANS [19].

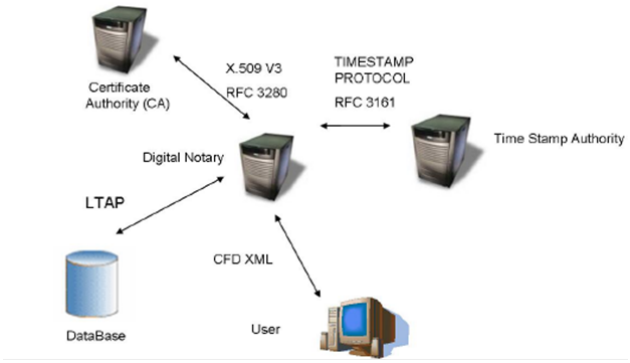

Figure 3. Digital Notary Architecture

6 Conclusion

In this paper we have identified a number of mild/serious problems when using the SAT´s specification for Digital Signature and digital invoices. In particular, there is a problem which requires the immediate attention of SAT, namely, the specification of sending taxpayers' private keys and passwords through Internet. Furthermore, the secure storage of those documents, should be taking into account by the digital invoice users. We have suggested some solutions to those and other problems pointed out througout the paper.

Acknowledgment

The first author acknowledges support from CONACyT project number 45306-Y. The second author acknowledges support from CONACYT under grant 60240. Third author acknowledges support from SIP-IPN 20072170.

References

[1] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). RFC 3161, IETF, Aug. 2001.

[2] Cámara de Diputados del H. Congreso de la Unión. Código Fiscal de la Federación, artículo 29 (in Spanish), December 2006.

[3] Cámara de Diputados del H. Congreso de la Unión. Código Fiscal de la Federación, artículo 30 (in Spanish), December 2006.

[4] S. de Administración Tributaria. SAT(México). Internet page. `http://www.sat.gob.mx`.

[5] I. E. T. Force. Public-key infrastructure X.509 PKIX, 2001. `http://www.ietf.org/html.charters/pkix-charter.html`.

[6] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2003.

[7] R. Housley, W. Ford, T. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, Apr. 2002.

[8] A. Jerman-Blazic and P. Sylvester. Long-Term Archive Protocol (LTAP) Draft-IETF-LTANS-LTAP-00. Internet Draft, 07 2005.

[9] B. Kaliski and J. Staddon. Rfc2437: Pkcs #1: Rsa encryption, October 1998. Available at: `http://www.ietf.org/rfc/rfc2437.txt`.

[10] R. Kuhn, V. Hu, T. Polk, and S.-J. Chang. Introduction to public key technology and the federal PKI infrastructure. *NIST*, February 2001.

[11] R. Laboratories. PKCS #7: Cryptographic Message Syntax Standard. Technical Note PKCS7, RSA Laboratories, Nov. 1993.

[12] R. Laboratories. PKCS #8: Private-Key Information Syntax Standard. Technical Note PKCS8, RSA Laboratories, Nov. 1993.

[13] R. Laboratories. PKCS #1 v2.1: RSA Cryptography Standard. Technical Note PKCS1, RSA Laboratories, June 2002.

[14] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560, IETF, June 1999.

[15] K. Schmeh. *Cryptography and Public Key Infrastructure on the Internet*. John Wiley & Sons, 2003.

[16] Secretaría de Hacienda y Crédito Público. Diario Oficial de la Federación de México, anexo 20 (in Spanish), September 1st 2004.

[17] Secretaría de Hacienda y Crédito Público. Diario Oficial de la Federación de México, regla 2.22.8 (in Spanish), May 31th 2004.

[18] Secretaría de Hacienda y Crédito Público. Diario Oficial de la Federación de México (in Spanish), Jun 28th and December 27th 2006.

[19] I. Secretariat. Long-Term Archive and Notary Services. `http://www.ietf.org/html.charters/ltans-charter.html`.

[20] W. Stallings. *Cryptography and network security*. Prentice Hall, 1998.