On the Security of Mexican Digital Fiscal Documents
De la Seguridad de Documentos Fiscales Mexicanos

Vladimir González García[1], Francisco Rodríguez Henríquez[2] and Nareli Cruz Cortés[3]
[1]National Laboratory on Advanced Informatics, LANIA A.C.
vlasland2@hotmail.com
[2]Computer Science Department, CINVESTAV-IPN
francisco@cs.cinvestav.mx
[3]Center for Computing Research (CIC)
National Polytechnic Institute (IPN), México
nareli@cic.ipn.mx

Article received on March 31, 2008; accepted on June 20, 2008

Abstract
In January 2005, the Mexican Tributary Administration System (SAT) introduced an official norm that stipulates how to generate electronic invoices that were termed by SAT, Comprobante Fiscal Digital (CFD). Supporting the CFD service implies the exchange of confidential information over Internet and other communication channels that are intrinsically highly vulnerable. Therefore, it becomes indispensable to incorporate to this service reliable and sound information security mechanisms. In the case of SAT's CFD, its security guarantees depend on customary cryptographic mechanisms such as, digital signatures, hash functions, etc. In this paper we point out several security flaws in the procedure specified by SAT for generating such electronic invoices. Furthermore, we provide recommendations for avoiding the security problems detected, which include the usage of more robust cryptographic mechanisms, alternative authentication protocols, time stamps authorities and a safe storage system.
Keywords: Information Security, Digital Certificates, Digital Notary, Mexican Tributary Administration System.

Resumen
En enero de 2005, el Gobierno mexicano a través del Servicio de Administración Tributaria (SAT), presentó una norma oficial que estipula cómo generar facturas electrónicas, las cuales recibieron el nombre oficial de Comprobante Fiscal Digital (CFD). El hecho de ofrecer el servicio de CFD implica el intercambio de información confidencial que debe viajar por Internet y otros canales de comunicación que son intrínsecamente altamente vulnerables. Por lo tanto, es indispensable incorporar a dicho servicio, herramientas de seguridad confiables y técnicamente sólidas. En el caso de los comprobantes fiscales digitales del SAT, su seguridad depende de mecanismos criptográficos tradicionales tales como, firmas digitales, funciones picadillo, etc. En este artículo se señalan fallas de seguridad en el procedimiento especificado por el SAT para la generación de sus facturas electrónicas. Aunado a esto, en este trabajo se dan algunas recomendaciones para eliminar los problemas de seguridad detectados, lo cual incluye, el uso de mecanismos criptográficos más robustos, protocolos de autentificación alternativos, autoridades que emitan estampillas de tiempo y un sistema de almacenamiento a largo plazo seguro.
Palabras clave: Seguridad informática, certificados digitales, notaría digital, servicio de administración tributaria.

1 Introduction

The concept of e-Government can be informally defined as the government's use of information technologies to exchange information and services with citizens, industries and other branches of government. The main goal of the e-government is to improve the internal efficiency, and to promote the prompt delivery of public services associated to democratic governance. In Latin-America, several countries have established the jurisprudence necessary to regulate governmental/commercial transactions made through the Internet. For example, Puerto Rico established its normative since 1998. That step was followed by Colombia in 1999, México and Perú in 2000, and Argentina and Venezuela in 2001.

In México, the normative called Norm-151 [NOM-151 Gobierno Mexicano, 2002] was introduced by the Mexican government on June 4, 2002. Norm-151 specifies the procedure to be followed for achieving the

confidentiality and integrity security services in official/sensitive documents. With the purpose of certifying documents' exact generation date, it was also suggested to use a cryptographic mechanism called Digital Time Stamping (DTS). It is worth mentioning that Norm-151 did not specify how to use the DTS mechanism [Hernández-Luna, 2007]. Further, since January 2005 the Mexican Tributary Administration System, (SAT after its name in Spanish) has offered to taxpayers a system for the automatic generation of electronic invoices, known as (*factura digital*) or Comprobante Fiscal Digital (CFD).

The CFD service is intended for automatizing the accounting process of individuals and enterprises, which is done by allowing Internet access to fiscal and administrative services. Up to this date, using CFDs is not mandatory, however, this service will be declared compulsory by SAT in a near future [SAT Secretaría de Hacienda y Crédito Público, 2008]. Since 2005, the CFD service has gradually gained a greater importance, among other reasons, because of the increasing number of Mexican enterprises that want to achieve an automatic accounting process. Only in the Mexican federal government case, the list of its branches and its decentralized dependencies that regularly 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*, among others. Moreover, from January 5, 2005 until December 31, 2007; a total of 9778 taxpayers had used the CFD service, 6980 of them being regular taxpayers ("Personas Físicas"), and 2798 being company representatives ("Personas Morales"). In addition, a total of 14,769,775 CFDs have been issued so far by the Mexican government [SAT Secretaría de Hacienda y Crédito Público, 2008].

It is noticed that SAT's CFD service implies the exchange of confidential information over communication channels that are intrinsically highly vulnerable. Therefore, 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, digital signatures may provide 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, replay attacks, identity usurpation, and so on [Schmeh, 2003]. Other potential devastating problems include the lack of protection against senders/receivers that refuse to acknowledge that they have sent/received a given document.

Because of the above, CFDs incorporate the usage of an infrastructure able to overcome aforementioned security gaps. That infrastructure is known as Public Key Infrastructure (PKI) [Kuhn et al., 2001]. Nevertheless, the PKI system is useless for establishing when a digital signature was generated. Knowing the exact date and time associated to the electronic invoice generation is, more often than not, crucial for commercial and/or legal transactions. This key feature, i.e. certifying when a given document was created, can be achieved by means of digital time stamping which in turn implies the usage of Time Stamp Authorities.

The main contributions of this paper are the following. We first present a careful analysis of the security protocols associated to SAT's Electronic invoice service. Then, we list major security flaws found by our study in SAT's specifications. Thereafter, we recommend several modifications to the current SAT protocols that can help to remedy the weaknesses detected. Finally, we present a system that guarantees secure storage of all the CFD created by an enterprise and/or individual. Our solution consists of a digital notary architecture that includes time stamp authorities as a mechanism to enforce digital time stamping.

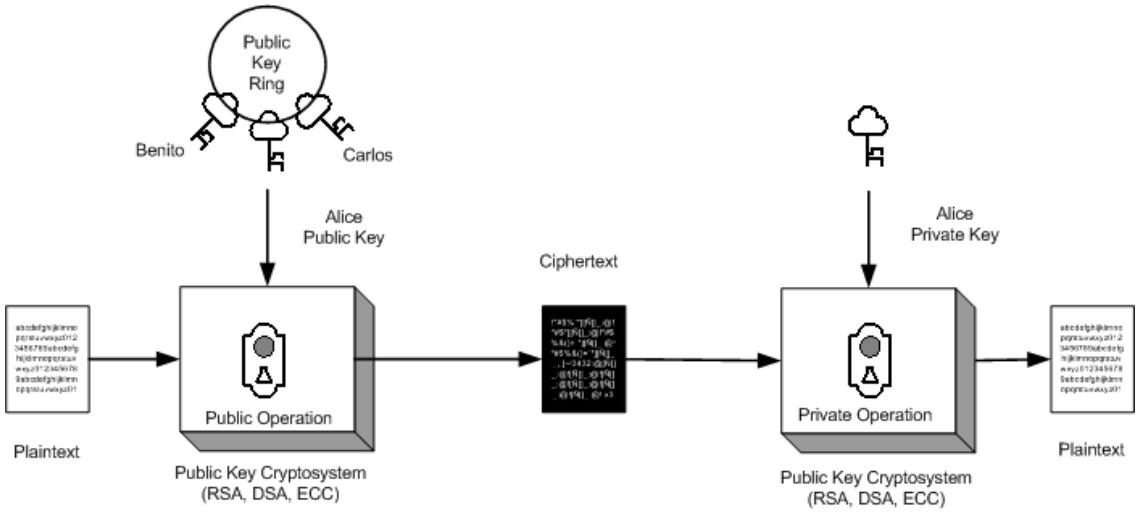

Fig. 1. Public Key Encryption/Decryption

The rest of this paper is organized as follows. In Section 2 we briefly summarize the most important security information concepts and services to be used throughout this manuscript. Then in Section 3 we outline the main procedures included in SAT's advanced digital signature FIEL protocol. In Section 4 we point out several security flaws in the FIEL protocol, whereas in Section 5 we give security solutions to the problems detected. The design specifics of a safe storage architecture is described in Section 6. Finally, in Section 7, concluding remarks are drawn.

2 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 to 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, in principle, cannot be forged. Roughly speaking, a digital signature should exhibit the following three properties,

1. Integrity: It implies that the received document is a genuine identical copy of the one that was sent.
2. Identity: It ensures that the received document was created by a given author.
3. 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 the CFD of a given provider. First, the sender must sign the hash value of the so-called *original chain*[1] by using his/her private key. Thereafter both, the original chain and its signed hash value are sent to the receiver. The receiver can then verify the CFD's signature by using the sender's public key that can be obtained from the provider's FIEL certificate as shown in Fig. 2. Only if the received original chain is identical to the one that was sent and if the correct public key (the one corresponding to the private key that was used for signing) is utilized, the signature will pass the verification process.

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 int the following four types [Schmeh, 2003]:

[1] The original chain is a summary of all relevant information contained in a CFD. For more details, the reader is referred to Section 3.4.

1. Secure Key Authentication. It is crucial to avoid attacks like man-in-the-middle, replay attacks and identity usurpation attacks among others.
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 public key Cryptography using the so-called Public Key Infrastructure (PKI) [Kuhn et al., 2001].

The de facto X.509 PKI [Housley et al., 2002; X.509 Internet Engineer Task Force, 2001] and PKCS [Kaliski and Staddon, 1998] 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) into a single security architecture. The main responsibility of a CA is to issue digital certificates to its users and to publish and maintain a Certificate Revocation List (CRL).

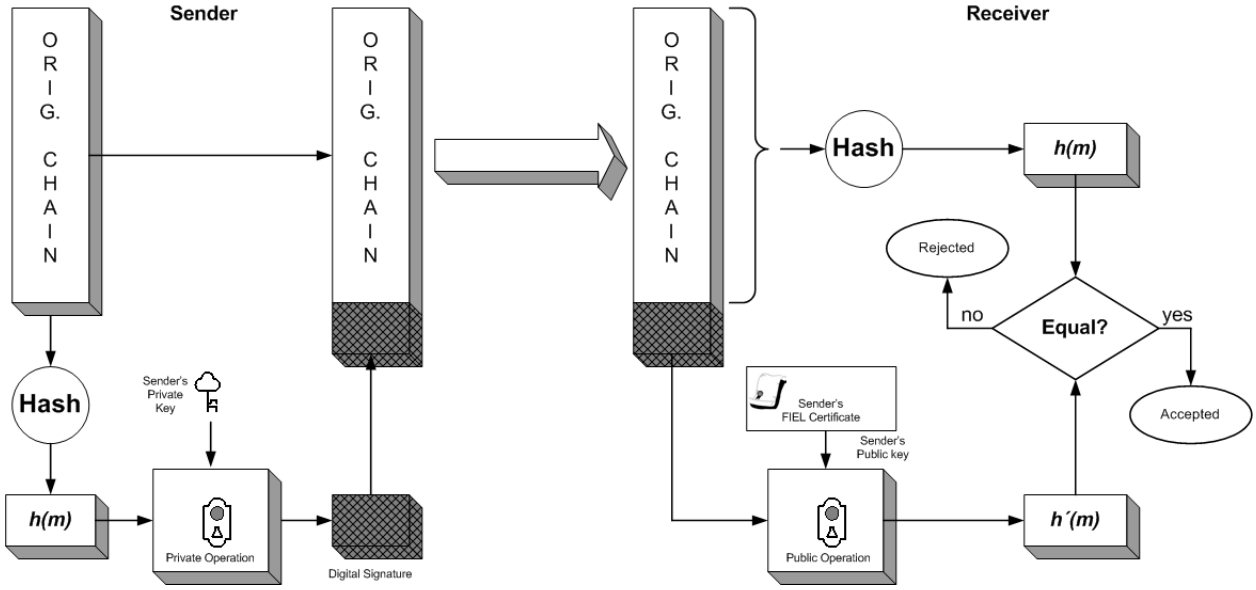

Fig. 2. Digital Signature/Verification

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. A digital certificate is used as a token-based identification method [Martínez-Silva et al., 2007]. Accurate user identification is essential to offer a reliable access control security service. In the case of SAT's CFD

service, a PKI based on the PKCS Standards [PKCS 7 RSA Laboratories, 1993; PKCS 1 RSA Laboratories, 2002] was adopted [SAT Secretaría de Hacienda y Crédito Público, 2008]. [2]

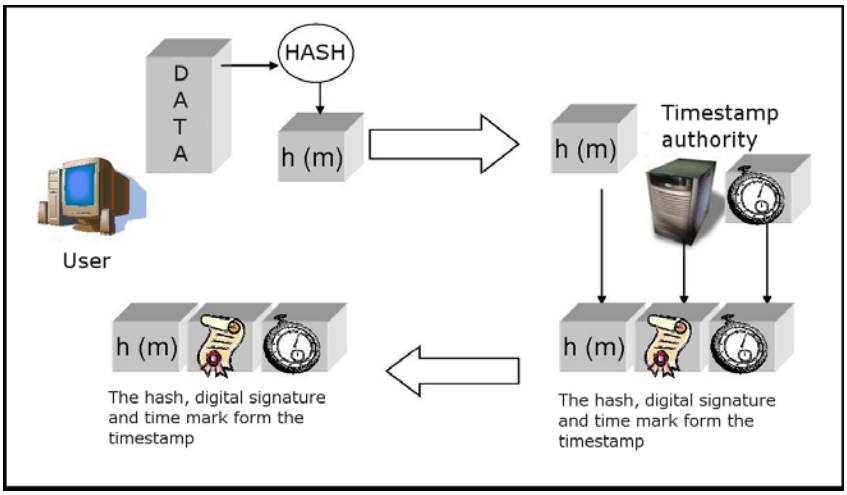

Fig. 3. Time Stamping a Document

2.1 Digital Time Stamps

Digital time stamping can be defined as the generation of a digital certificate that guarantees the existence of a generic digital document before a particular time and that it has not been modified since then [Gabillon and Byun, 2001; Haber and Stornetta, 1990; Haber and Stornetta, 1991; Haber and Stornetta, 1997; Massias et al. 1999]. Time stamping schemes can be classified into two main classes, namely, those based on distributed trust, and those that rely on a trusted third party [Gabillon and Byun, 2001]. The former model is based on the notion that if a document has been dated and signed by a large number of users, then the verifier entities can get convinced about the authenticity of such signatures (due to the low probability that all such users have been corrupted or compromised by the adversary). The latter model is based on the impartiality of the Time Stamp Authority, the entity that is in charge of issuing the time stamps. Clearly, techniques based on distributed trust cannot be applied in the context of SAT's CFDs. Hence, in the rest of this document we will only focus on the model of a trusted third party authority.

A Digital time stamp must meet the following criteria [González-García, 2007; Haber and Stornetta, 1990; Haber and Stornetta, 1991; Haber and Stornetta, 1997],

- The time stamp must be embedded within the document being time stamped.
- Any document and/or time stamp modification should be detected.
- It should be computationally infeasible to insert in the document a date and/or hour different than the authentic one.

In order to achieve the characteristics mentioned above, the following solutions have been proposed [Haber and Stornetta, 1997],

1. Refereed Solution: A copy of each document that has been time stamped by the Authority is stored in a master database.

[2] In México there exist five major PKI systems [Hernández-Luna, 2007]. All five of them have been implemented by the following governmental organisms, the Mexican Tributary Administration System (SAT), Banco de México, the Mexican Economy Ministry, the Mexican Health System (IMSS after its name in Spanish) and the Mexican Internal Affair Ministry. In addition, the organism, *Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico*, was created on December 9, 2005 in order to promote a PKI standardization within México [Acuerdo Gobierno Mexicano, 2005].

2. Improved Refereed Solution: Similar to the one above, but in this case, is the hash of the document the one that gets time stamped and stored.
3. Linked Protocol: The authority time stamps and signs the hash of the document. In addition, the time stamp is linked with the last one issued. This way if a given time stamp is modified, then all the time stamps that were issued afterwards, will also get altered.
4. Distributed Protocol: Several Time Stamp Authorities act together issuing partial time stamps. Then, the one authority that originally received the user's request produces the complete time stamp by combining all the partial stamps [Takura et al., 1999].

The X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) in [Adams et al., 2001] defines a Time Stamp Authority (TSA) as a Trusted Third Party that provides a proof-of-existence for a particular datum at an instant in time. This can be used to verify that a digital signature was applied to a message before the corresponding certificate. Other natural application of a TSA is to establish the time of submission when a deadline is critical, or to indicate the time when the transactions of a protocol took place.

The steps specified in this protocol in order to produce a valid time stamp are outlined in Fig. 3. As shown in Fig. 3, we first obtain the hash value of the document to be time stamped. Then, the TSA generates a certificate that contains the hash, the time and the signature of the Time Stamp Authority. Additionally, it is strongly recommended that time-stamping information should be obtained soon after the signature has been produced, for example, within a few hours. In order to verify the correctness of a time stamped document, the following procedure is performed,

- Check if the hash received and the one obtained from the document are the same or not. If yes then,
- Check if the certificate was indeed issued by the Time Stamp Authority. If yes then,
- Compare the time stamp date and time against local references. If they agree then,
- Verify that the state of the certificate is not revoked.

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

The Advanced Electronic Signature [3] (FIEL after its name in Spanish), is the implementation of a digital signature based on the PKI standard specified in [Kaliski and Staddon, 1998]. According to the Mexican Federal Fiscal Code published in [SAT Secretaría de Hacienda y Crédito Público, 2008], every taxpayer must require his/her FIEL. Up to this date, however, for some services the usage of the FIEL is optional.

In Mexico, an electronic invoice is a legal digital document with fiscal validity that follows the standards defined by SAT [Anexo 20 SHCP Secretaría de Hacienda y Crédito Público, 2006]. 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 [SAT Secretaría de Hacienda y Crédito Público, 2008].

In the rest of this Section we will describe the security architecture utilized by 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.

3.2 Key Generation and Digital Certificate 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 [PKCS 8 RSA Laboratories, 1993] and ciphered according to the standard PKCS#1 [PKCS 1 RSA Laboratories, 2002]. The private/public key can be obtained through an application developed by SAT

[3] "*Firma Electrónica Avanzada*".

which is available at the Internet called SOLCEDI (after its name in Spanish: *solicitud de certificados digitales*). SOLCEDI is an application directly written from the primitives defined in the open-source library OPENSSL [Young and Hudson, 2007], 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 [Housley et al., 2002] generated by 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 using its private key. According to the procedure specified by SAT, a user FIEL certificate can only be granted before SAT's officers. 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, CD or USB memory.

3.3 Folios

Taxpayers must request the approval of electronic folios by SAT, which are composed by a series number and a single 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 requests for folios consist of 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 [PKCS 7 RSA Laboratories, 1993] 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 [Schmeh, 2003]. Once the folio certificate has been obtained it is possible to request for folio approvals.

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 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 that includes all the relevant data of the invoice as it has been defined and published in [Anexo 20 SHCP Secretaría de Hacienda y Crédito Público, 2006]. The original chain should be generated under the standard UTF-8.[4]
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 [PKCS 1 RSA Laboratories, 2002], this signature process ensures that the digital invoice was signed by the legitimate owner of the private key. The resulting signature should be encoded 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. Thereafter, the signature verification is done by extracting the certificate's public key.

3.5 CFD Format

The generation, decoding and storing of a CFD as a digital invoice must follow the XML format. Version 1 and 2 of this format was published in [Anexo 20 SHCP Secretaría de Hacienda y Crédito Público, 2006], any of these two versions can be used. The XML format defines fields containing fiscal data. Any additional information (such as

[4] According to SAT's terminology, the original Chain corresponds to "*Cadena original*" in Spanish.

commercial information, barcodes, number of purchase, discounts, special offers, time stamp, etc.) can be inserted into the invoice within a field called "addenda".

3.6 Monthly Report

Every month, the folios that have been utilized must be reported. Currently, this monthly report must be done through SAT's web page (SICOFI). Monthly reports 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 [Anexo 20 SHCP Secretaría de Hacienda y Crédito Público, 2006]. This report must be signed by SAT through the module SICOFI.

3.7 Communication with SAT

At present date, it is necessary to have a direct connection to 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, it has not been released.

3.8 Printing the Electronic Invoice

In [Regla 2.22.8 SHCP Secretaría de Hacienda y Crédito Público, 2004], SAT establishes that, in addition to the requirements published in [Artículo 29 Cámara de Diputados del H. Congreso de la Unión, 2006], 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*".[5]

3.9 Storage

Every generated and/or received invoice must be stored in its original format XML. In [Artículo 29 Cámara de Diputados del H. Congreso de la Unión, 2006] 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 worth noticing that the data stored should be physically located into the user's fiscal address as registered by SAT, otherwise, if for some reason this were not the case, then the user should notify SAT immediately.

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 important issue.

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 Internet connections or by visiting SAT's offices with the corresponding documents and credentials [SAT Secretaría de Hacienda y Crédito Público, 2008].

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) [Housley et al., 2002], it is necessary to access SAT´s WEB page [SAT Secretaría de Hacienda y Crédito Público, 2008]. SAT should implement a WEB service called on line Certificate Status Protocol (OCSP) as specified in [Myers et al., 1999], so that taxpayers can perform on-line queries investigating which certificates have been revoked. Once again, this service was projected to appear at 2005, however, it has yet to be released.

[5] "This document is a digital fiscal invoice printed copy".

4 Problems

In this Section we briefly outline the security flaws that our analysis detected in SAT's electronic invoice system.

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 inputting in the system the taxpayer federal register value (RFC by its acronym in Spanish: "*Registro Federal del Contribuyente*") and a pre-agreed password.

In the case of the FIEL certificate authentication, SAT's user identification module asks 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. Moreover, 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, replay attacks, etc. 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 SAT´s system must be corrected immediately, because it denies privacy to all the taxpayer Mexican citizens.

4.2 Data 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, Hence, it is perfectly possible to change the actual CFD's date and time at any moment, even without 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, an attacker can launch several devastating attacks against the system as discussed in for example [Stallings, 1998].

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 ones created legally. Things can get 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.

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 [Artículo 30 Cámara de Diputados del H. Congreso de la Unión, 2006]. 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. Therefore, 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.

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

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

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.
- 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 SAT's WEB page using the session key.

Those steps would only require that a program executed at the taxpayer side decrypts SAT's challenge by applying his/her private key.

5.2. Digital Fiscal Documents Generation

A Time-Stamp Authority certifies that the registered time and date have not suffered any modification. The service given by this authority may be operated as a Trusted Third Party (TTP) [Adams et al. 2001; Haber and Stornetta, 1997]. The X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) [Adams et al., 2001] defines a time-stamp authority, specifies the service requirement, the type of answer to be given, the errors, the security methods to be used, data structures and the certificate authority requirements. A time-stamp service is capable of processing verification requirements, that is, it verifies that a data existed in a determined date and time. If a time-stamp server is used, it can 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 [Rodríguez-Henríquez et al., 2006].

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 [Hankerson et al., 2003]), 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 one 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.

To that end, it is possible to use a client-server architecture as the one shown in Figure 4. The Digital Notary may archive all digital invoices and digital certificates using Evidence Record Syntax (ERS) and the communication protocol LTAP [Jerman-Blažiĉ, 2007; Jerman-Blažiĉ, 2005] defined by the working group LTANS [LTANS IETF Secretariat, 2008].

In the Next Section we describe an architecture that can emulate SAT's CFD system and at the same time, can provide safe storage for the datum being manipulated.

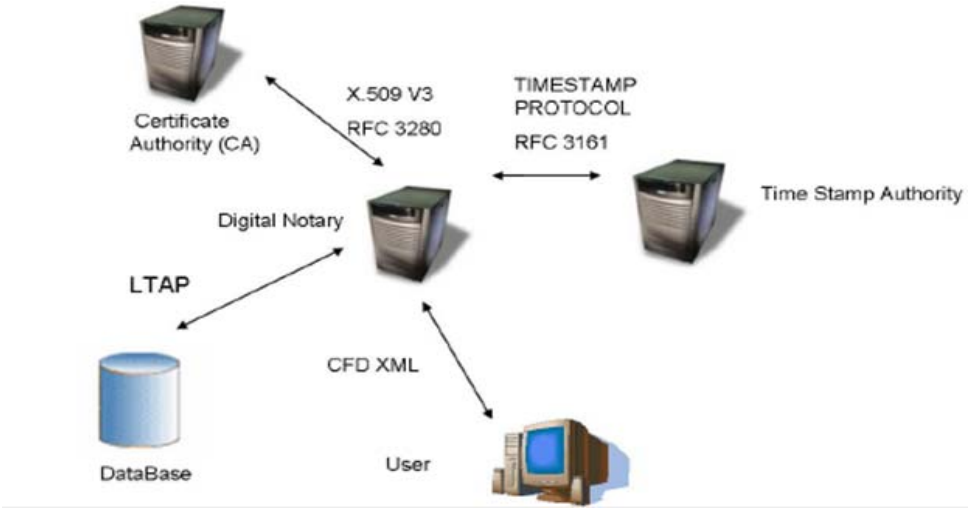

Fig. 4. Safe Storage Architecture

6 Implementation

In this Section we describe the main building blocks of the safe storage architecture implemented in this work, which are shown in Fig. 4. We also explain how our system can be integrated to an emulated SAT's CFD system (See Fig. 5). Our system was coded in the C and C++ programming languages. It allows the correct generation and safe storage of certified CFDs and it also permits to verify their validity. The CFDs are generated in XML format, fully-complying with the XSD format specified by SAT. The certified CFDs can be long-term stored for as long as required by SAT (a period of time of 5 years is typical, however, sometimes documents must be stored for up to 10 years). As shown in Fig. 5, the complete system is composed by the following main modules,

- Safe Storage Module.
- CFD Generator Module.

- Certificate Authority.
- Time Stamp Authority.
- Database.

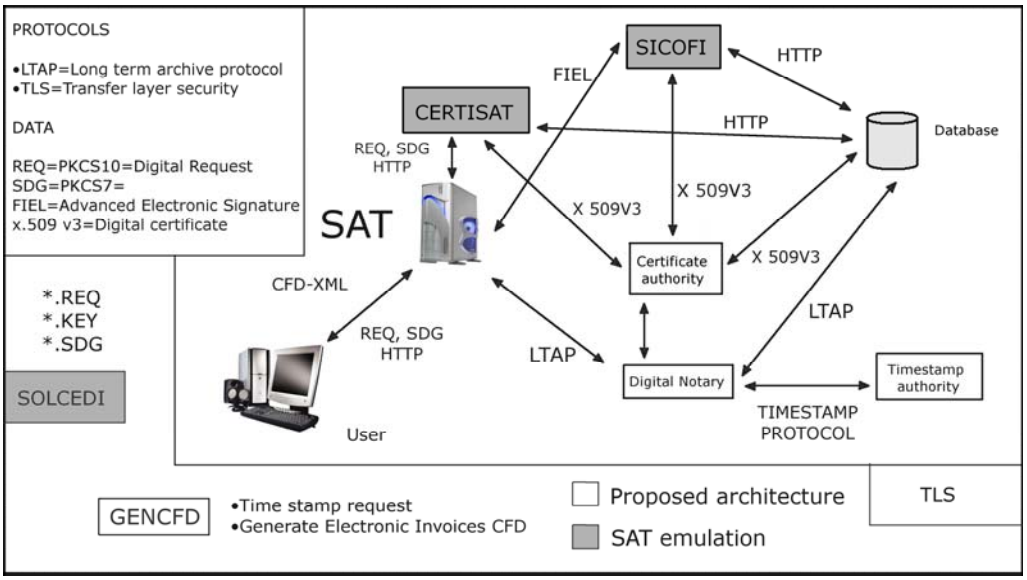

Fig. 5. An Architecture that Emulates SAT's CFD System with A Safe Storage System

6.1 Safe Storage Module

Based on the LTAP protocol [Jerman-Blažič, 2005], this module is responsible of getting "Proof of Evidence" for all the CFD generated by the system. In our implementation, the Safe Storage Module utilizes a client-server communication. It works as an independent module that exchanges information with the Certification and Time Stamp Authorities and it can read/write to/from the main database. It supports the minimum set of services defined in [Jerman-Blažič, 2005], namely, Storage, Status, Verification, Export and Deletion of CFDs. The system uses an Apache WEB server, which allows communication with any client that supports the HTTPS protocol.

6.1.1 CFD Generator Module

In order to generate a CFD, our CFD generator module performs the following steps,

1. It writes all CFD relevant data in XML format according to the XSD format specified by SAT.
2. It generates the original chain that is to say, the hash value of the CFD data obtained in the previous step.
3. It requests to the Time Stamp Authority (TSA) a time stamp for the original chain document generated in the previous step.
4. It retrieves the time-stamped document and it adds to it, the official date and time granted by the TSA.
5. Using the CFD extension field addenda, it adds the time stamp of the previous step to the XML document of Step (1).
6. It signs the XML document of the previous step using its private key. The signature is stored in the field termed by SAT "Sello Digital".
7. The time stamped CFD so obtained along with the digital certificate of the CFD generator module is sent to the requester (Safe Storage Module).
8. The Safe Storage Module records the existence of a new document and it stores it in the database.

6.2 Certification Authority

This module is responsible of implementing the PKI system. It generates, revokes and manages x.509v3 digital certificates. Additionally, it is also responsible of publishing the Certificate Revocation List (CRL) periodically. In our architecture this module was implemented using the OpenSSL library [Young and Hudson, 2007].

6.3 Time Stamp Authority

As it was explained in Subsection 2.1, The TSA is responsible of providing proof-of-existence for a particular datum at a given instant in time. In our implementation, the TSA receives the hash value of the document to be time stamped. It returns a document that includes the received hash value, along with the corresponding time stamp and TSA signature of the first two values. The time stamp is formatted according to the ASN.1 [Dubuisson, 2000].

6.4 Database

The database stores all the proof of evidence of the CFD documents generated by the system. It can be accessed by the Certification Authority and the Safe Storage Module. This module was implemented in MySQL DBMS.

7 Conclusion

In this paper we have identified a number of mild/serious problems when using SAT's Digital Signature and digital invoice specifications. In our opinion, the most serious problem, which requires the immediate attention of SAT, is the authentication protocol that obligates taxpayers to send their corresponding private keys and passwords through Internet. This procedure should be eliminated at once from SAT's CFD system and substituted for authentication protocols that help to confirm private key possession.

Another important problem is the lack of a Certificate Revocation List periodically published by SAT. This makes impossible for regular taxpayers to detect revoked certificates, and this, can easily bring disastrous situations in commercial transactions. Furthermore, according to Mexican laws, CFDs should be stored for as much as 10 years. This makes the cryptographic suite specified by SAT designers a dangerous choice. This is especially true for the RSA-1024 bit public key system and the MD5 hash function, which are already broken or soon will be.

We also recommend to extend the CFD specification so that secure storage and CFD time stamping is also included. To this end, in this paper we presented the design specifics of a Safe storage architecture that can fully comply with SAT's CFD specification while, at the same time, it allows the usage of digital notary and digital time stamps concepts.

Acknowledgments

The second author acknowledges support from CONACYT under grant 45306. The third author acknowledges support from CIC-IPN.

References

1. **Acuerdo Gobierno Mexicano**, "Acuerdo que tiene por objeto crear en forma permanente la comisión intersecretarial para el desarrollo del gobierno electrónico" (in Spanish). In Diario Oficial de la Federación, December, 9 2005.
2. **Adams C., Cain P., Pinkas D., and Zuccherato R.**, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". RFC 3161, IETF, August 2001. Available at: http://www.ietf.org/rfc/rfc3161.txt.
3. **Anexo 20 SHCP Secretaría de Hacienda y Crédito Público**, "Anexo 20 de la resolución miscelánea fiscal para 2006" (in Spanish). Diario Oficial de la Federación de México, September 1st 2006. Available at: http://www.sat.gob.mx/nuevo.html.
4. **Artículo 29 Cámara de Diputados del H. Congreso de la Unión**, "Artículo 29 del Código Fiscal de la Federación". In El Diario Oficial de la Federación, Gobierno de México. (in Spanish), December 2006.

5. **Artículo 30 Cámara de Diputados del H. Congreso de la Unión**, "Artículo 30 del Código Fiscal de la Federación". In El Diario Oficial de la Federación, Gobierno de México. (in Spanish), December 2006.
6. **Dubuisson O.**, "ASN.1 Communication Between Heterogeneous Systems". Morgan Kaufmann Publishers, 2000. http://asn1.elibel.tm.fr/en/book/.
7. **Gabillon A. and Byun J.**, "A two-level time-stamping system". In Sec '01: Proceedings of the 16th international conference on Information security: Trusted information, pages 139–149, 2001.
8. **González-García V.**, "Diseño y desarrollo de un prototipo de notaría digital" (in Spanish). Master's thesis, Laboratorio Nacional de Informática Avanzada LANIA, August 2007.
9. **Haber S. and Stornetta W. S.**, "How to time-stamp a digital document". In A. Menezes and S. A. Vanstone, editors, CRYPTO, volume 537 of Lecture Notes in Computer Science, pages 437–455. Springer, 1990.
10. **Haber S. and Stornetta W. S.**, "How to time-stamp a digital document". J. Cryptology, 3(2):99–111, 1991.
11. **Haber S. and Stornetta W. S.**, "Secure names for bit-strings". In ACM Conference on Computer and Communications Security, pages 28–35, 1997.
12. **Hankerson D., Menezes A., and Vanstone S.**, "Guide to Elliptic Curve Cryptography". Springer, 2003.
13. **Hernández-Luna F. A.**, "Análisis e implementación de la norma oficial mexicana NOM-151-SCFI-2002". Propuesta de Tesis de Maestría, Programa de Graduados en Ciencias Computacionales. Instituto tecnológico y de estudios superiores de Monterrey, Zona metropolitana de la Ciudad de México, December 2007.
14. **Housley R., Ford W., Polk T., and Solo D.**, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 3280, IETF, Apr. 2002. Available at: http://www.ietf.org/rfc/rfc3280.txt.
15. **Jerman-Blažič A., Klobučar T., and Donova-Jerman B**, "Long-term trusted preservation service using service interaction protocol and evidence records". Comput. Stand. Interfaces, 29(3):398–412, 2007.
16. **Jerman-Blažič A. and Sylvester P**. "Long-Term Archive Protocol (LTAP)", draft-ietf-ltans-ltap-06. Internet Draft, August 2005. Available at: http://tools.ietf.org/html/draft-ietf-ltans-ltap-06.
17. **Kaliski B. and Staddon J.**, "RFC2437: PKCS #1: RSA Encryption", October 1998. Available at: http://www.ietf.org/rfc/rfc2437.txt.
18. **Kuhn R., Hu V., Polk T., and Chang S.-J.**, "Introduction to public key technology and the federal PKI infrastructure". NIST, February 2001. Available at: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.
19. **LTANS IETF Secretariat**, "Long-Term Archive and Notary Services (LTANS)". Available at: http://www.ietf.org/ html.charters/ltans-charter.html. abril, 2008.
20. **Martínez-Silva G., Rodríguez-Henríquez F., Cruz-Cortés N., and Ertaul L**, "On the generation of x.509v3 certificates with biometric information". In S. Aissi and H. R. Arabnia, editors, Security and Management, pages 52–57. CSREA Press, 2007.
21. **Massias H., Avila X. S., and Quisquater J.-J.**, "Timestamps: Main issues on their use and implementation". In WETICE, pages 178–183. IEEE Computer Society, 1999.
22. **Myers M., Ankney R., Malpani A., Galperin S., and Adams C.** "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP". RFC 2560, IETF, June 1999.
23. **NOM-151 Gobierno Mexicano**, "Norma oficial mexicana NOM-151-SCFI-2002, prácticas comerciales, requisitos que deben observarse para la conservación de mensajes de datos" (in Spanish). In Diario Oficial de la Federación, June, 4 2002.
24. **PKCS 1 RSA Laboratories**, "PKCS #1 v2.1: RSA Cryptography Standard. Technical Note PKCS1", RSA Laboratories, June 2002. Available at: http://www.ietf.org/rfc/rfc3447.txt.
25. **PKCS 7 RSA Laboratories**, "PKCS #7: Cryptographic Message Syntax Standard. Technical Note PKCS7", RSA Laboratories, Nov. 1993. Available at: http://www.ietf.org/rfc/rfc2315.txt.
26. **PKCS 8 RSA Laboratories**, "PKCS #8: Private-Key Information Syntax Standard". Technical Note PKCS8, RSA Laboratories, 1993.
27. **Regla 2.22.8 SHCP Secretaría de Hacienda y Crédito Público**, "Regla 2.22.8" (in Spanish). Diario Oficial de la Federación de México, May 31th 2004.

28. **Rodríguez-Henríquez F., Saqib N. A., Díaz-Pérez A., and Koç Ç. K.**, "Cryptographic Algorithms on Reconfigurable Hardware". Springer, First Edition, November 2006.
29. **SAT Secretaría de Hacienda y Crédito Público**. Servicio de administración tributaria. Internet WEB page. Available at: http://www.sat.gob.mx.
30. **Schmeh K.**, "Cryptography and Public Key Infrastructure on the Internet". John Wiley & Sons, 2003.
31. **Stallings W.**, "Cryptography and network security". Prentice Hall, 1998.
32. **Takura A., Ono S., and Naito S.**, "A secure and trusted time stamping authority". In 1999 Internet Workshop, IWS 99, Osaka, Japan, pages 88–93, february 1999.
33. **X.509 Internet Engineer Task Force**, "Public-key infrastructure X.509 PKIX", 2001. Available at: http://www.ietf.org/html.charters/pkix-charter.html.
34. **Young E. A. and Hudson T. J.**, "The OpenSSL Project", December 2007. Available at: http://www.openssl.org/.

Vladimir González García *received the Master degree (2007) in Computer Science from the* National Laboratory *on Advanced Informatics* LANIA *A. C., in Xalapa, Veracruz, Mexico and the B.Sc. (2005) degree in Computer Science and Bussines Administration both from the University of Veracruz, Mexico. His major research interests are Computer Security and Information Systems.*

Francisco Rodríguez Henríquez *received the PhD (2000) degree in Electrical and Computer Engineering from Oregon State University, the M.Sc. (1992) degree in Electrical and Computer Engineering from the National Institute of Astrophysics, Optics and Electronics (INAOE), México and the B.Sc. (1989) degree in electrical engineering from the University of Puebla, México. His major research interests are in data security, cryptography, finite fields, error correcting codes, and mobile computing. He is a member of the IEEE and he is also an alumni member and research associate of the Information Security Laboratory at Oregon State University.*

Nareli Cruz Cortés *received the PhD degree (2004) in Electrical and Computer Engineering from CINVESTAV, Mexico, the Master M.Sc. (2000) degree in Artificial Intelligence from the University of Veracruz and the LANIA, Veracruz, Mexico and the B.Sc. (1995) degree in Computer Engineering from the Technological Institute of Tepic, Nayarit, Mexico. Currently, she holds an associated professor position in the Center for Computing Research of the Polytechnical National Institute (CIC-IPN). Her major research interests are in Combinatorial and Multiobjective Optimization, Evolutionary Computation and Heuristics applied to Information Security.*