A Secure E-transaction Model for E-commerce

Dalila BOUGHACI and Habiba DRIAS

University of Sciences and Technology – USTHB
BP 32, El-Alia Beb-Ezzouar, 16111, Algiers, Algeria
Dalila_info@yahoo.fr

Abstract— **Electronic commerce is an Internet-based business transactions performed electronically by individuals, companies, corporations and governments utilizing information and communication technologies. The most important obstacle to further expansion for e-commerce has been the lack of adequate security protections. When sending secure data via the Web, four items, no provided by Internet, are needed: confidentiality, Integrity, Authentication, and non-repudiability. This paper describes them, briefly summarizes some relevant cryptographic technologies and proposes a novel cryptographic- based model to support a secure e-commerce. More precisely, our proposed model uses XML combined with cryptographic techniques to create a secure session between partners in which the traffic between the partners is encrypted and only the adequate participants can decrypt it, to transmit structured data across the Web and to further improve the security of the exchanged documents.**

Index Terms — **ecommerce, secure transaction, cryptography, XML, XML encryption, XML decryption.**

I. INTRODUCTION

E-commerce can be viewed as a means of interchanging goods and services using Internet technology [7, 2]. The latter makes it possible to improve inter-organizational process. However, a lack of adequate security protections is an inherent problem of Internet network. There are a wide variety of potential attacks which may be mounted by malicious or third no authorized parties. They break down into passive attacks in which communications are only monitored or active attack, in which communications are subverted [5]. In addition, e-commerce attackers can be classified in two categories: external attackers, who may attempt to listen in or modify message, or act under false identity. Insiders' attackers related to misbehaving business partners [10].

In order to improve e-business security, many utilities such as digital signatures, encryption/authentication and SSL [6] have been proposed and important progress has been achieved. SSL can be used to encrypt data and sent it securely across the Web but what is much more interesting is how to handle situations where different parts of the same document need different treatments. This can not be done by using only SSL.

Nowadays, XML is widely used to transmit structured data across the Web; the security of such documents is becoming a necessity. As a solution, the Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF) have proposed a XML security suite technology in 1999 [15] and continue working on it. This new technology includes XML digital signature, XML encryption, XML decryption and other utilities. It provides essentially a non-repudiability function.

For all arguments cited above, we try to propose a novel transaction model using XML combined with cryptographic techniques to achieve confidentiality, integrity, authentication and non-repudiability security services and handles situations where different parts of the same document need different treatments. Notice that, the security of a session between partners is preserved with the use of cryptographic techniques while the security of documents exchanges is ensured by the XML combined with cryptographic mechanisms. Our proposed e-transaction model is started by creating a secure session between partners using cryptographic mechanisms, then a secure negotiation phase is launched between the business parties using the secure key generated in the pervious step; the goal of the negotiation step is to negotiate the items to be exchanged (contract, goods, etc). Finally, in last phase of the model, the secure XML document can be exchanged between business parties. The security of the document is preserved with the use of XML security suite in particular XML signature and XML encryption.

The rest of this paper is organized as follows: section 2 provides a brief overview of cryptographic techniques. Our proposed model is described in detail in section 3. The last section concludes our work and draws the future one.

II. SOME USEFUL CRYPTOGRAPHIC TECHNIQUES

The goal of this section is to introduce the main modern cryptographic techniques. Definitely, cryptography is the

science of the enciphering and deciphering of messages in secret or cipher.

The main services offered by the modern cryptography are [1, 12]:

- Confidentiality: assures that the concerned data will be able to be unveiled only to the allowed people.
- Integrity: assures that data won't be tampered (deliberately or no) during their transmission or their storage. The data isn't altered as it goes from the sender to the receiver.
- Authentication:/identification: proves the origin of a data or a person's identity.
- Undeniability / non-repudiation: Signing cleanly so-called permits to a person to take part to a contract with impossibility to disown its engagements.

Some historic references of the modern cryptography are: [12, 1]

- 1975. Conception of D.E.S Data Encryption Standard, adopted in 1977,
- 1978. Invention of R.S.A, the first public key cryptosystem.
- 1985. Invention of the system El-Gamal
- 1991 Adoption of the first standard of signing, ISO 9796, based on RSA,
- 1994 Adoption of DSS, digital signature standard based on El-Gamal.

The cryptography techniques can be classified in two categories symmetric and asymmetric cryptosystems according to the type of keys to be used.

A. Symmetric Encryption:

The symmetric cryptography technique works with a single key; why it is often called private or a single key cryptography. Its cryptosystem takes plaintext (P) and converts it to ciphertext (C), given the same key (K) it also converts ciphertext (C) back into plaintext (P).

Mathematically, we can write: **C= K (P)**. The ciphertext is computed from the plaintext via a function of the key (K) and the reverse also works: **P = K (C)**.

The most well-known private key algorithm in the world is the Data Encryption Standard DES [9]. DES has a 64-bit block size and uses a 56-bit key encryption. DES is a 16 –round Fiestal cipher and was originally for implementation in hardware. It is based on the same secret key used to encrypt and decrypt the message [9]. For further information about DES and other private cryptosystems such as triple DES, IDEA, you can refer to [12, 1].

B. Asymmetric Encryption:

The Asymmetric cryptography technique is called public key system. With such techniques, each user has two keys: a public key and a secret key. The public key is public, it can be published. The secret key is never shared.

The system functions as follow:

Let consider A, a sender and B, a receiver two users.

- The user A encrypts a message to B by computing: **$C = K_{PB}(P)$, $_{PB}$ is a B's public key.**
- To decrypt, B computes **$P = K_{SB}(C)$, $_{SB}$ is a B's secret key.**

One encrypted, A cannot decrypt the resulting message. B is the only one capable to decrypt the encrypted message using the secret key.

The most well-known public key algorithm and widely used in the world is RSA. It has often been referred as a de-facto standard regardless of official recognition. It has been invented in 1978 by Ron **R**iverst; Adi **S**hamir and Leonard **A**dlmen. [11]

The method is as:

Let consider p and q two prime numbers, n=p*q

- We chose two big numbers d and e as: e is prime with $(p-1)*(q-1)$, $e < n$ and $d = e^{-1}$.
- The encrypted number, C, is computed from the original number $M < n$ as**:** $\mathbf{C = M^e \bmod (n)}$
- The encrypted number back into the original number by: $\mathbf{M = C^d \bmod (n)}$

We note that the couple (n, e) is the public key and the couple (n, d) is the secret key. El-Gamal is also one of the most well-known public key algorithms. It is based on the discrete logarithm. For more details about the public key cryptography techniques you can refer to [4, 8].

C. Cryptographic Hashes**:**

The cryptography hash technique permit to known whether some message has been tampered with, without having to transmit a copy out of band. MD5 and secure hash algorithm SHA are examples of cryptographic hash algorithms. These one-way hash functions compute a short (128 bit) message digest of the original long message, with the property that changing any single bit of the original message changes, on average, half of the bits of the digest [5]. They are often used to implement digital signature since signing a hash is much faster then signing the original long message.

The cryptographic techniques provide confidentiality which means that third parties cannot read the message. Authenticity which means that receiver can proves that a

sender, A, sent the message, how? The response is given by this example:
Let consider A, a sender and B, a receiver two users, where:

$_{SA}$ is the A's secret key,
$_{PA}$ is the A's public key,
$_{SB}$ is the B's secret key,
$_{PB}$ is the B's public key.

Before A sends a message, he first signs the message by encrypting it using cryptographic hash technique with his own private key.
- A computes, then, $P_{signed} = K_{SA}(P)$,
- A encrypts the message to B, computing:

$$C = K_{PB}(P_{signed})$$

- B upon receiving the message computes:

$$P_{signed} = K_{SB}(C)$$

Which recovers the plaintext and he can verify A's signature by computing: $P=K_{PA}(P_{signed})$.

III AN OVERVIEW OF THE PROPOSED APPROACH:

In this section we show how to implement a secure e-transaction for doing business on the Web. Our framework makes use of cryptographic techniques and XML –related security to support a secure e-commerce.
The proposed e-transaction model depicted on figure1, below, can be decomposed into four main levels.

1-Certified Authentication level**,**

2-Secure session creation level**,**

3-Negotiation level**,**

4- XML documents exchanges level**.**

The security of the first three levels is guaranteed through the use of cryptographic techniques while the security of document is assured with the use of XML-related security. The e-transaction model is started by creating a secure session between partners using cryptographic mechanism, then a secure negotiation phase is launched between the business parties using the secure key generated in the pervious step; the goal of the negotiation step is to negotiate the items to be exchanged. A negotiation mechanism is designed to enable interactions between partners. The goal is to reach an agreement. The exchanged items can be: E-contract, E-goods, E-services, E-payment, etc. Finally, in last phase of the model, the secure XML document can be exchanged between business parties. The security of the document is preserved with the use of XML security suite in particular XML signature and XML encryption.

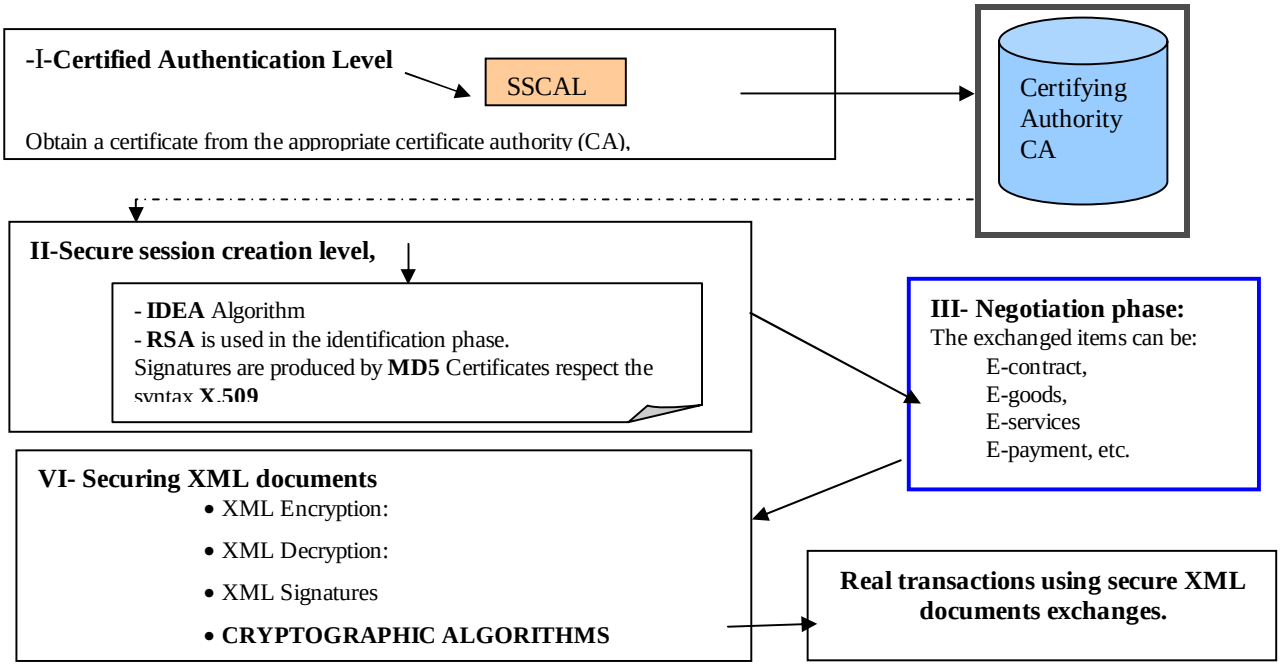

Fig.1. A secure e-transaction model.

A. Secure Session Certified Authentication Layer

The Secure Session Certified Authentication Level, SSCAL, has been developed to offer security and confidentiality on Internet. This protocol permits to identify clients and servers in a socket connection type. It is an intermediate layer of the communication protocol level session, which is not bound to any particular application. Therefore it permits to secure all existing protocol of Internet application; which are: http, ftp or telnet and that, without modifying the software.

How SSCAL works?

At the beginning of the session, the SSCAL protocol identifies the server, the client, and then negotiates parameters of encryption. During the session, SSCAL ensures confidentiality and the reliability of exchanges using cryptographic techniques and identification of messages. During the identification phase, the server sends its certificates and indicates its cryptographic algorithms. After that, the client generates a first key so-called "main key" or "pre-master key". Then, he encrypts it with the server's public key before sending it to the server. The server has recognized himself by returning a message encrypted by the "main key". Exchanges that follow are encrypted by the key derived from the "main key". The client's identification is optional. The server sends to the client any message and the client will be identified by returning his electronic signature on this message, accompanied of his certificates. SSCAL manage signatures only on messages foreseen in the phase of identification. SSCAL uses IDEA cryptographic algorithm [3, 6]. RSA is used in the identification phase. Signatures are produced by MD5. Certificates respect the syntax X.509 [13].

B. XML documents exchanges level

In the last years, XML (Extensible Markup Language) has become a valuable mechanism for data exchange across the Internet. XML is a simplified dialect of the language SGML (ISO 8879), that provides a format of file to represent data, a diagram to describe the structure of data and a mechanism to enrich and to annotate the HTML language [14]. As XML is widely used to transmit structured data across the Web, the security of documents becomes increasingly important. Thus, a new technology in XML security has been proposed in 1999 by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) [15]. These technologies are based on open, emerging standards as RSA and DES and they work on any Java-enabled platform. The new technology, XML security suite, provides a variety of functions that enhance the security of XML documents. It includes XML digital signature, XML encryption, XML decryption and other utilities. Note that SOAP (Simple Object Access Protocol) is the means of sending XML messages that facilitates process intercommunication [15]. After having created a secure session between partners using the proposed SSCAL protocol, the XML documents exchanges between partners can be started. The security of documents is ensured via the use of XM security suite. Our choice is justified in the next section.

Why XML Security Suite?

Secure protocols as SSL, SET, or our proposed SSCAL protocol can be used to encrypt data and sent it securely across the Web. But what is much more interesting is how to handle situations where different parts of the same document need different treatments. For example, in a binary business transaction between vendor and customers, the vendor may need to know some information related to customer as his name and his address. This information can be transmitted clearly across the Web. But he does not need to know various details about his credit card. As a solution XML Security suite contains utilities that automatically generate XML digital signature, provide element-level encryption. It also provides a means of dealing with the particular requirements of security as they apply to XML documents [15]. Below, we introduce three important functions which are XML signing, XML encryption and XML decryption may be used to improve the security of XML document. We give later some interesting examples based.

XML Encryption:

Data to be encrypting may be an XML document, an XML element, or XML element content. The result of encrypting data is an XML encryption *"EncryptedData"* element which contains or references the cipher data. The *"EncryptedData"* element has the following structure:

```
<EncryptedData  Id ? Type? Mime Type? Encoding ?>
   <EncryptionMethod / > ?
    <ds: KeyInfo>
         <EncryptedKey> ?
         <AgreementMethod  > ?
         <ds: Keyname>?
         <ds: RetrievalMethod>?
         <ds: *>?
</ds: KeyInfo>

    <CipherData  > ?
        <CipherValue > ?
         <Cipherreferences URI ? > ?
     </ CipherData  >
     <EncryptionProperties> ?
 </EncryptedData >
```

Where: ? denotes zero or one occurrence,
* denotes one or more occurrences,
empty element tag means the element must be empty.

The <CipherData> element envelopes or references the raw encrypted data. So, the encrypted data is the <Ciphervalue> element content. If referencing the <*Cipherreference*> elements URI gives the reference to the encrypted data.

XML Decryption:

It is also possible to convert the encrypted XML document back into the original XML document with the use of XML decryption. .

In order to obtain the unencrypted XML document, for each *Encryptedtype*, (EncryptedData / EncryptedKey) the decrypt or must be launched:The decryption process follows these steps:

- processes the element to determine the algorithm, parameters and key information element to be uses
- decrypts the data encrypted key
- decrypts data contained in cipher data element

XML Signatures:

The main benefit of digital signature is that it provides non-repudiability. If we send a signed document, the receiver knows that I am the sender because the signature contains my public key. The XML signatures are a XML element <*signature*> that contains all the information necessary to process a digital signature. A digital signature can refer to an XML element contained inside the <*signature*> element, an external XML document, referenced by a URI, it can refer also to an external non-XML resource, referenced often by a URI [15. 20].

C. An example of a secure e-Transaction scenario

Let consider two business parties A and B (for example A, a vendor and B a customer) and also the existence of a certification authority (CA).

In the first level, business parties mutually authenticate each other and agree on a session key that will be used. How this can be achieved?

To create a secure session, we may use the SSCAL mechanism and follows these steps:

1- the party A obtains a certificate from the appropriate certificate authority (CA),

2- the party A sends its public key to the party B,

3- the party B uses the party A's public key to encrypt a pre-master secret,

4- the party A uses its private key to decrypt the pre-master secret

5- the party A generate a new key based on the pre-master secret. The key is know to the party A and can only be decrypted and used by the party B that generates the pre-master secret This five steps permit to create a secure session between the two businesses parties A, which offers the service and B, which demand the service. The communications are encrypted and only the two parties are capable to decrypt each other's data. The negotiation level is then launched between partners in order to negotiate the content of business. The last level is the exchanges of the secure XML documents. It is the execution of business process between the two parties using XML standard documents.

V CONCLUSION

In this work, we have described some relevant cryptographic techniques. We have used XML technology to encode messages with meaningful structure and semantics, and cryptographic techniques to create a secure session between partners in which the traffic between the business parties is encrypted and only the adequate participants can decrypt it. We have also combined XML with cryptographic utilities to further improve the security of e-transaction on the Web. That may provide an effective support to implement a secure e-commerce. We plan, in a future work, to add on our proposed model an agent technology to automate some business tasks.

REFERENCES

[1] Annault, F, "Théorie des nombres et cryptographie"; *Internet document;* 2002.

[2] Boughaci D and Drias, H. " Taboo Search as an Intelligent Agent for Bid Evaluation", *in International journal of Internet and Enterprise Management*, inderscience Publisher, Vol 3 issue 2, pp 170-186, spring 2005.

[3] Caprani L, "paiement sur Internet", université du Québec à Monté real; Avril 1996.

[4] El-Gamal, T. "A public-key cryptosystem and a signature scheme based on discrete logarithms", *in IEEE transactions on Information theory*, *IT-31* pp 469-472, 1985.

[5] Foner L, "A security architecture for multi-agent matchmaking", the first international conference en multi-agent ICSMA'96; 1996.

[6] Hickam, "The protocol SSL", *KEB* December 1995.

[7] Junho shim, "Roadmap for e-commerce standardization in Korea", *in proceeding of CE2003*, pp329-334, 2003.

[8] Lai, X, Massey J.L and Murphy.S, "Markov ciphers and differential cryptanalysis". *In advances in cryptology*-EUROCRYPT'91, pp17-38, 1991.

[9] NBS, "National Bureau of Standards, Data Encryption Standard DES", Federal information prodessing standards, publication N 46, Washington DC:USNBS, 1977.

[10] Nenadic. A, Zhang.N, Barton.S, "A secure and fair DSA-based signature exchange protocol", in proceeding of ITCC'04; IEEE computer society, 2004.

[11] Riverst, Shamir and Adleman, "RSA data security", Inc's home page.

[12] Schnier, Bruce, "Applied cryptography: protocols, algorithms and source code in C", *second edition, Joh wisely and sons*, 1996.

[13] X509, "CCITT recommendation X.509", the directory-Authentication framework, 1988.

[14] http://www.xml.org

[15] http://www.w3c.org

[16] www.w3c.org/2001/04/xmlenc#tripledes-cbc

[17] www.w3c.org/2001/04/xmlenc#aes128-cbc

[18] www.w3c.org/2001/04/xmlenc#RSA-1_5

[19] www.w3c.org/2001/04/xmlenc#DHKeyvalue

[20] www.w3c.org/2000/09/xmldsigc#SHA1