DESIGN OF A SECURE FINE-GRAINED OFFICIAL DOCUMENT EXCHANGE MODEL FOR E-GOVERNMENT

Yi-Hui CHEN and Eric Jui-Lin LU

Abstract: At present, the exchange of information via Internet is widely used in electronic government (e-Government). To securely and effectively exchange official documents among government agencies, an exchange model has been developed by the government of Taiwan. Although a RSA cryptosystem is used in the model to ensure security and XML is employed to increase interoperability, the current design does not take advantage of the rich structure of the XML documents, and it may result in possible security leaks due to the fact that, traditionally, the whole document is signed and encrypted. Considering the characteristic that it is easy to integrate encryption, signature and access control into XML documents, a fine-grained official document exchange model for e-Government is proposed in this article. In addition, the proposed model conforms to standards such as XML Encryption and XML Signature.

Keywords: e-Government, XML Encryption, XML Signature, Document Exchange.

The global acceptance of electronic commerce and the progress made in network technologies have great impact on the development of electronic government (e-Government). One of the main objectives of e-Government is to exchange information between government agencies in a timely manner.[1,2,3] In Taiwan, the e-Government program was initiated in 1997.[4] During the first phase of the program, Taiwan established the country's first certification authority – the Government Certification Authority (GCA). From 2001 until 2004, one of the major applications of the e-Government program enabled the secure and effective exchange of official documents between governmental agencies. As a result, an exchange model has been developed.[5,6,7] In the model, as illustrated in Figure 1, an official document is first transformed into XML format;[8,9] then the XML-based document is signed and encrypted; and finally the encrypted document is sent to the Official Document Exchange Center. Next time when the recipient logs in, the ciphered document will be retrieved

INFORMATION & SECURITY. An International Journal, Vol.15, No.1, 2004, 55-71.

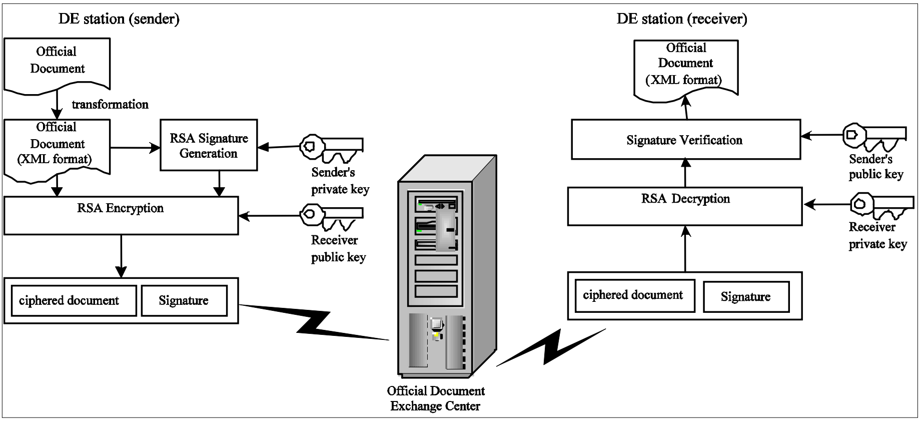
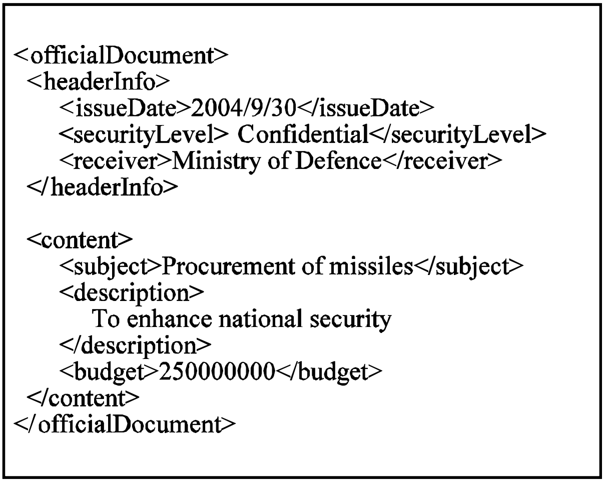


Figure 1: An Official Document Exchange Model.

from the center. The received ciphered document will then be decrypted and verified in order to obtain the original document.

Although the Rivest-Shamir-Adleman (RSA) cryptosystem[10] is used to ensure security and XML is employed to increase interoperability in the model, the current model does not take advantage of the rich structure of the XML documents and may result in possible security leaks due to the fact that, traditionally, the whole document is signed and encrypted. For example, in the current implementation, each agency assigns a specialized staff to send and receive official documents. When an official document, classified as “confidential,” is received, the staff is still able to decrypt the whole document and read its content even though s/he is not authorized. Therefore, it is very important to design a secure official document exchange model with fine-grained control so that only designated recipients are allowed to read and process the received documents, while the staff that receives the incoming documents is only allowed to verify their validity.

To achieve these objectives, it is required that the official document contains all the information needed for encryption, signature, and access control. Traditional security mechanisms, in view of the fact that the target of access control is usually the whole document, require more than one file to accomplish these tasks. Fortunately, due to the rich structure of XML, *it is easy to integrate encryption, signature, and access control into one XML document*. Therefore, this article proposes a fine-grained official document exchange model for e-Government. Taking advantage of the rich structure of XML, the content of the XML documents can be encrypted at various security levels.[11] Example of an official document is given in Figure 2. The official document has two parts – header information and content of the document. The header indicates that the document was issued on 2004/09/30, the official document is classified as “confidential,” and the recipient is the Ministry of Defense. The body of the document describes the budget that is required to purchase missiles to enhance national security. The staff at the receiving desk will be able to read the header information of the received document. However, since the arriving document is classified as “confidential,” s/he will not be able to read the content of the document. Instead, only the designated staff is allowed to decrypt and read the document.



```
<officialDocument>
 <headerInfo>
     <issueDate>2004/9/30</issueDate>
     <securityLevel> Confidential</securityLevel>
     <receiver>Ministry of Defence</receiver>
 </headerInfo>

 <content>
     <subject>Procurement of missiles</subject>
     <description>
         To enhance national security
     </description>
     <budget>250000000</budget>
 </content>
</officialDocument>
```

Figure 2: An Official Document Example.

The proposed model conforms to standards such as XML Signature[12] and XML Encryption.[13] The content of an official document can be encrypted by different keys based on the security level. And the staff can only decrypt and read the content of the document if s/he is authorized. In addition, due to the fact that the RSA cryptosystem is adopted in the proposed model, it is secure and can be easily incorporated into existing implementations.

The rest of the paper is organized as follows. First, a smartcard-based framework for secure document exchange, the XML Encryption, an XML Multi-signature scheme, and the XML Signature are briefly reviewed. Then the design of the secure fine-grained official document exchange model is described in detail. Afterwards, the authors analyze and summarize the advantages of the proposed model. Finally, some conclusions are provided in the last section.

Related Work

A Smartcard-Based Framework for Secure Document Exchange

A secure document exchange model was proposed by Yang, Ju, and Rao.[14] There are many Document Exchange (DE) Stations and a Security Management Center in the model, as shown in Figure 3. Each DE Station is responsible for sending and receiving documents and equipped with a smart card reader. Cryptographic algorithms are embedded in the smart card to provide security functions for digital signature and digital envelope. The Security Management Center is responsible for issuing smart cards, acting as a public-key certificate authority, regularly publishing certificate revocation list, and maintaining distribution lists. A distribution list contains a group of recipients that can be used as a mailing list to send and receive official documents.

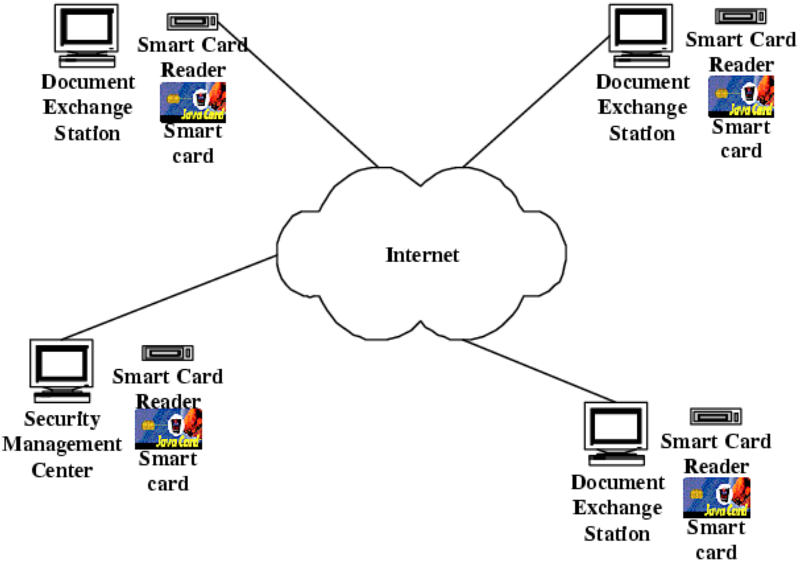


Figure 3: Yang-Ju-Rao’s Secure Document Exchange Model.

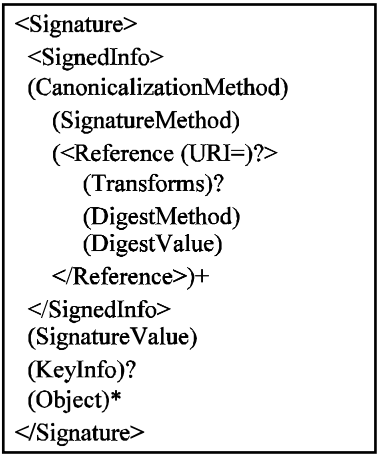
An official document is first transformed into XML format, and the XML-based document is then signed and encrypted. Unlike the current implementation used in the Taiwanese official document exchange system, the ciphered document and its signature are sent directly to the recipient. Upon receiving the ciphered document, the recipient decrypts, verifies, and obtains the original document. Although the Yang-Ju-

Rao’s model is secure and XML is also adopted, there is still a possibility for security leaks. The reason is identical to the one in the official document exchange model used by the government of Taiwan.

XML Signature

For ensuring the authenticity and the integrity of the data transmitted over the Internet, digital signature techniques are widely adopted. If the signature is validated, the transmitted document is integral and authentic. The digital signature is based on public-key cryptography in conjunction with one-way hash functions. After creating a one-way hash value (called message digest) from the document, the signer encrypts the digest value with her/his private key. In the traditional signature techniques, every participant signer signs the whole document rather than these portions of the document that s/he is responsible for. This brings two major drawbacks.[15] One is that it requires extra communication cost to transfer the whole document and extra computation time to generate personal signatures on the whole document. The other drawback is that it is difficult to achieve the principle of responsibility separation. It is extremely time consuming and tedious to read the whole document before signing it. In practice, every signer should sign these parts of the document that s/he is responsible for. To overcome these drawbacks, Lu and Chen[16] proposed a novel XML multi-signature scheme in 2003 that provides fine-grained control at element level.

The W3C XML Signature Working Group has worked on a standard called XML Signature.[17] The standard provides key developments based on various security strategies to support that the signer can sign only portions of the document.



```
<Signature>
  <SignedInfo>
  (CanonicalizationMethod)
      (SignatureMethod)
      (<Reference (URI=)?>
           (Transforms)?
           (DigestMethod)
           (DigestValue)
      </Reference>)+
  </SignedInfo>
  (SignatureValue)
  (KeyInfo)?
  (Object)*
</Signature>
```

Figure 4: Structure of the XML Signature.

The XML structure for representing digital signatures is shown in Figure 4.[18] Every XML Signature is enclosed within a Signature element. In the Signature element, there are several main elements including a SignedInfo element that contains all the information about the signed data and additional information required for signature validation.

The information how to locate the data object, the algorithm to generate the digest, and the digest value are included in the Reference element. For instance, the hashing function can be described in the DigestMethod element, whereas the digest is stored into the DigestValue element.

The Reference element can also encompass a Transforms element that contains a list of transformations (i.e. one or more Transforms elements) used by the signer to transform a document into a set of sub-documents. For example, the Transforms element can contain an XPath expression to identify the selected portions within the document.

Before utilizing digital signature, the SignedInfo element is transformed into a standard form called *canonical form*. The role of the canonical form is to eliminate additional symbols, such as white spaces, to avoid errors during the signature validation process. The canonical algorithm is specified in the CanonicalizationMethod element. After the canonical form has been generated, it is then encrypted with the key of the signer. The final step is to compute the digital signature of the whole SignedInfo element and the resulting value can be written in the SignatureValue element. All the information about the algorithm used for generation of the digital signature of SignedInfo, such as the encryption algorithm, is saved in the SignatureMethod element. The Signature element can also provide information on the keys used to validate the signature to the recipient. A KeyInfo element contains the keys used to validate the signature.

The XML Signature draft supports three different types of signatures which are shown in Figure 5 [19]:

- *Enveloping Signature*: The Object element includes the data object; therefore, it is a part of the Signature element.
- *Enveloped Signature*: The data object encloses the *Signature* element. Therefore, the *Signature* element is inserted into the XML document embracing the data object being signed.
- *Detached Signature*: The data object is either an external data object, or a local data object included as a sibling element in the XML document containing the *Signature* element.

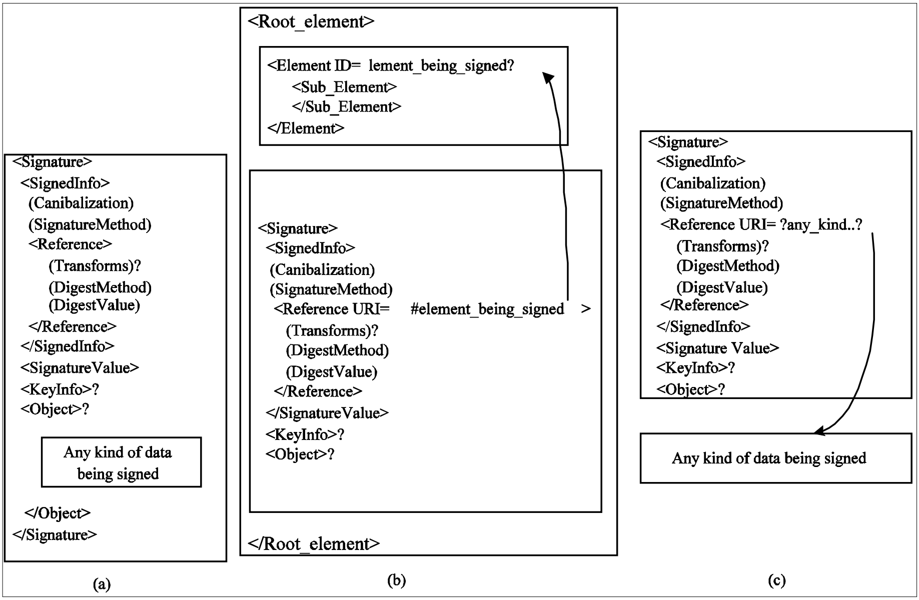


Figure 5: XML Signature Types: (a) Enveloping Signature (b) Enveloped Signature (c) Detached Signature.

An XML Multi-Signature Scheme

In the past, conventional multi-signature schemes allowed the participant signers to only sign on the whole document. This fact made the multi-signature schemes inefficient. To overcome the problem, Wu, Huang, and Guan[20] proposed a delegated multi-signature scheme in which the participant signers sign on the sub-documents that they are responsible for.

In Wu-Huang-Guan's delegated multi-signature scheme, a document is decomposed into a set of subdocuments and the subdocuments are assigned to qualified signers by means of a dispatch algorithm. There are four roles involved in this scheme: a group of signers, a system authority (SA), a document dispatcher (DD), and a signature collector (SC). SA provides services such as initialization of system parameters and generation of the secret and public keys for the individual users and the group. DD is responsible for document decomposition and sub-document delegation. SC collects and verifies the personal signatures generated by the delegated signers; it also constructs a multi-signature for the group. It is assumed that both SC and SD are trusted and only the cheating tricks plotted by DD are considered.

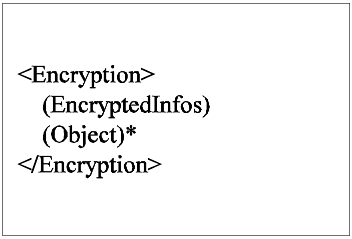
It is believed that XML is the *de facto* standard format for data interchange. To prevent the interchanged XML documents from being illegally modified or forged, digital signatures have to be incorporated in practical implementations.[21] Although software developers can directly apply Wu-Huang-Guan's multi-signature scheme or another multi-signature scheme to all XML documents, all of the schemes proposed so far do not consider the logical structure of XML and, thus, result in extra computation and communication overhead.

To overcome the described problems, an XML multi-signature scheme has been proposed by Lu and Chen.[22] The scheme is based on Wu-Huang-Guan's delegated multi-signature scheme and utilizes XPath, which is an official recommendation released by W3C, to transform an XML document into a set of sub-documents. In summary, the scheme inherits the advantages of Wu-Huang-Guan's scheme, further improves the efficiency in multi-signature generation by signing the rules rather than the sub-documents, provides fine-grained control at the element level, and is also compatible with the XML Signature standard.

XML Encryption

Various encryption techniques have been designed for encrypting a whole document, but they do not support selective encryption of a document. However, a requirement of many applications is that users have the ability to encrypt only selected portions within a document and encrypting different portions of the same document with different encryption keys. To meet this requirement, XML Encryption has been proposed by the W3C XML Encryption Working Group.[23] At time of writing, the XML Encryption is a working draft. It is mentioned in the draft that the granularity of encryption is limited to the element level as long as XML documents are concerned. Therefore, it is not possible to just encrypt selected attributes of an element.

An XML Encryption structure is composed of two parts and they are `EncryptedInfos` and `Objects`, as is illustrated in Figure 6. The information needed for a correct decryption is stored in the `EncryptedInfos` element, and the encrypted data are contained in the `Object` element.



```
<Encryption>
   (EncryptedInfos)
   (Object)*
</Encryption>
```

Figure 6: Structure of the XML Encryption.

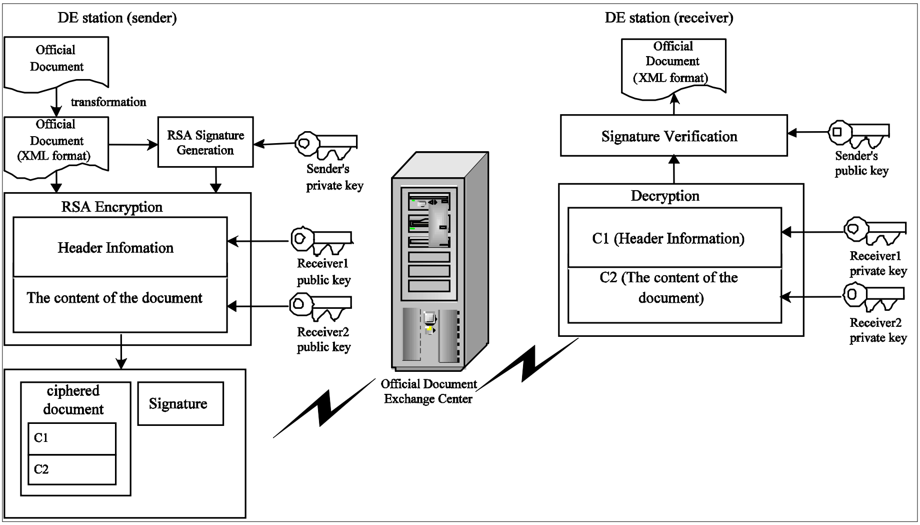
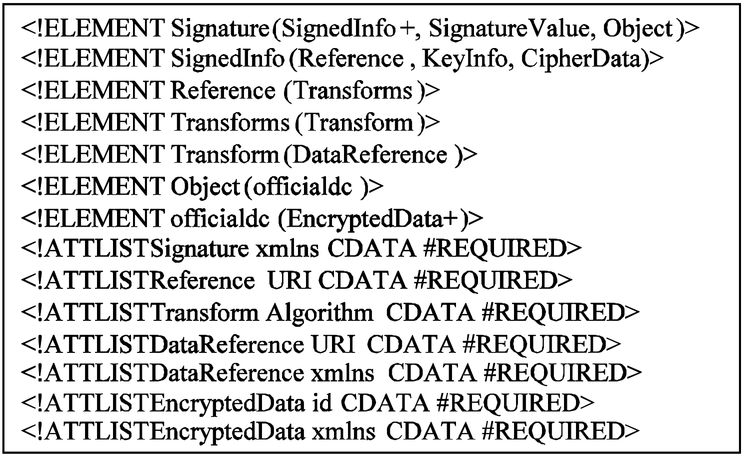


Figure 7: A Secure Fine-Grained Official Document Exchange Model.

Design of a Fine-Grained Official Document Exchange Model

The basic idea of the proposed model is that the originators or senders can sign and encrypt selective portions of a document with different keys based on the security policies. Therefore, only the designated recipients are allowed to read and process the received documents. A few issues have to be emphasized. First, the number of senders and the designated recipients can be one or more than one. Second, the granularity of the protected data object can be as small as a single element. This is due to the fact that any XML element or a set of XML elements can be identified by XPath[24] expressions. And last, the proposed model conforms to the XML Signature and the XML Encryption specification drafts.

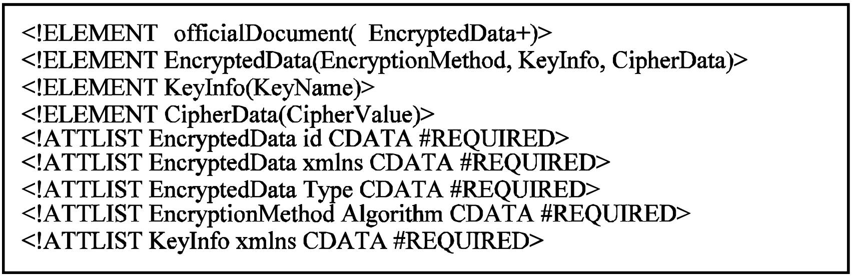
The proposed secure fine-grained official document exchange model is shown in Figure 7. The model includes one sender side, one official document exchange center, and more than one receiving sides. First, each recipient has to register at the official document exchange center and the registration information is stored in a database. The registration information includes at least the recipient’s name and her/his public-key certificate. Also, the role of the recipient in the government agency has to be registered. As stated earlier, for the reason that GCA has been established in Taiwan, all government agencies have their own public/private key pair. Additionally, with the roles employed in the proposed model, the management of recipients (or government agencies) is much easier.



```
<!ELEMENT Signature(SignedInfo+, SignatureValue, Object)>
<!ELEMENT SignedInfo (Reference , KeyInfo, CipherData)>
<!ELEMENT Reference (Transforms )>
<!ELEMENT Transforms (Transform )>
<!ELEMENT Transform (DataReference )>
<!ELEMENT Object (officialdc )>
<!ELEMENT officialdc (EncryptedData+ )>
<!ATTLISTSignature xmlns CDATA #REQUIRED>
<!ATTLISTReference  URI CDATA #REQUIRED>
<!ATTLISTTransform Algorithm  CDATA #REQUIRED>
<!ATTLISTDataReference URI  CDATA #REQUIRED>
<!ATTLISTDataReference xmlns  CDATA #REQUIRED>
<!ATTLISTEncryptedData id CDATA #REQUIRED>
<!ATTLISTEncryptedData xmlns  CDATA #REQUIRED>
```

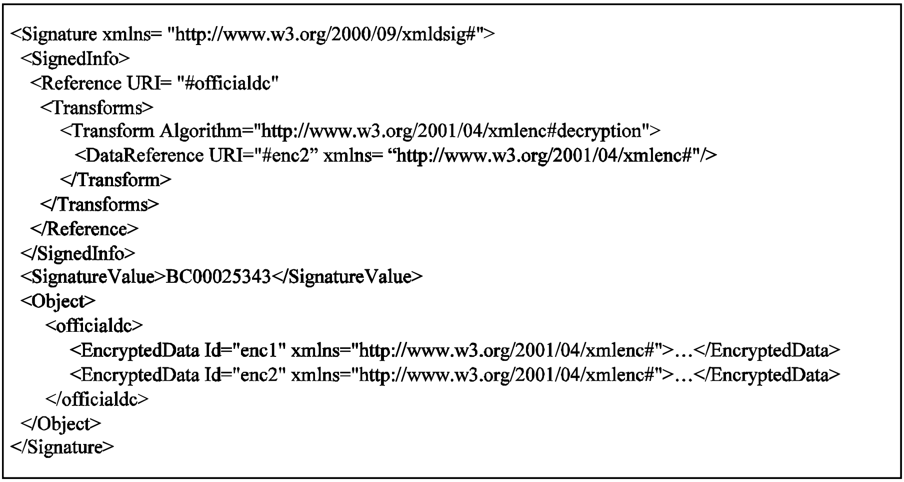
Figure 8: The DTD of Signature.

Prior to sending an official document to the recipients, the sender can retrieve the recipients' certificates from the database of the official document exchange center. Once the certificates are obtained, the sender can sign the official document with her/his private key and encrypt the selected parts of the document with the recipients' public keys. The encrypted document and its signature will then be sent to the document exchange center. Upon logging into the official document exchange center, the staff at the receiving desk will receive official documents addressed to her/him. The received encrypted document will first be decrypted and verified. If the document is verified successfully, the staff at the receiving desk can check the header information to see if s/he is permitted to process the document. If the document is classified as "confidential," the document will then be forwarded to the designated recipient.



```
<!ELEMENT   officialDocument(  EncryptedData+)>
<!ELEMENT EncryptedData(EncryptionMethod, KeyInfo, CipherData)>
<!ELEMENT KeyInfo(KeyName)>
<!ELEMENT CipherData(CipherValue)>
<!ATTLIST EncryptedData id CDATA #REQUIRED>
<!ATTLIST EncryptedData xmlns CDATA #REQUIRED>
<!ATTLIST EncryptedData Type CDATA #REQUIRED>
<!ATTLIST EncryptionMethod Algorithm CDATA #REQUIRED>
<!ATTLIST KeyInfo xmlns CDATA #REQUIRED>
```

Figure 9: The DTD of Encryption.



```
<Signature xmlns= "http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <Reference URI= "#officialdc"
   <Transforms>
     <Transform Algorithm="http://www.w3.org/2001/04/xmlenc#decryption">
       <DataReference URI="#enc2” xmlns= “http://www.w3.org/2001/04/xmlenc#"/>
     </Transform>
   </Transforms>
  </Reference>
 </SignedInfo>
 <SignatureValue>BC00025343</SignatureValue>
 <Object>
    <officialdc>
       <EncryptedData Id="enc1" xmlns="http://www.w3.org/2001/04/xmlenc#">…</EncryptedData>
       <EncryptedData Id="enc2" xmlns="http://www.w3.org/2001/04/xmlenc#">…</EncryptedData>
    </officialdc>
 </Object>
</Signature>
```

Figure 10: An Example XML Signature.

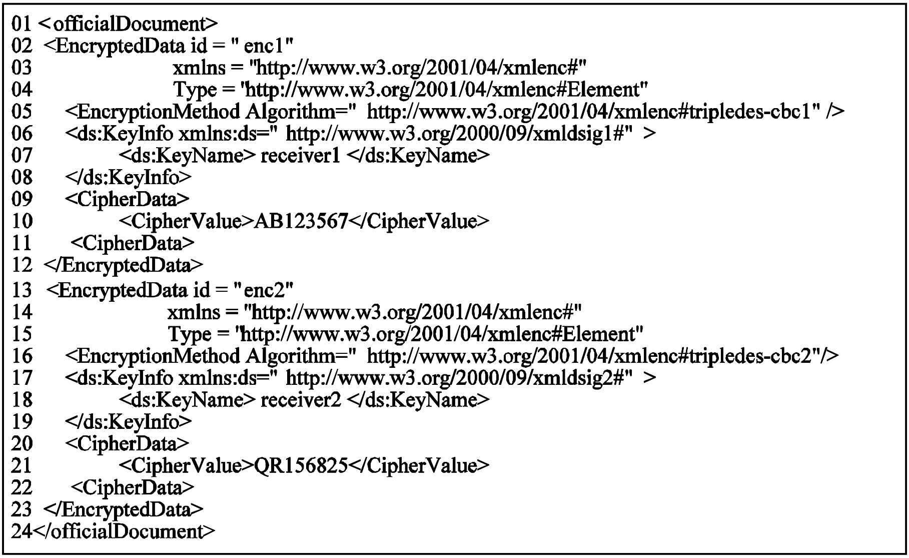
The signature and the encrypted document are encoded in XML, and their schemas are shown in Figure 8 and Figure 9, respectively. To keep the schemas as simple as possible, DTD has been chosen to describe the schemata. This should help in clarifying the concept. If necessary, the readers can choose the W3C XML Schema[25] to describe the schemata. In this article, the “enveloped signature” type of XML signature is adopted. The reason for this choice is that the schemata of the proposed model remains the same even when the structure of the official documents is revised. In Figure 8, the `officialdc` element is composed of more than one `EncryptedData` element, which are the ciphered sub-documents encrypted by a different security level. The `id` attribute of the `EncryptedData` element is used to establish the relationship between the signature and its associated encrypted document or sub-document. The value of the `id` attribute is unique for one official document. The `EncryptedData` element is composed of at least one `EncryptionMethod`, `KeyInfo`, and `CipherData` elements. The `EncryptionMethod` element has `Algorithm` attribute to specify the encryption algorithm. The `KeyInfo` element stores additional information enabling the recipient to obtain the keys for decryption. After a document or a sub-document is encrypted, the ciphered data is stored in `CipherData` element.

Consider for example that Bob wishes to send a confidential official document to Alice at the government agency “Ministry of Defense.” The person at the receiving desk of the Ministry of Defense is Tom. The official document is denoted as D; it is composed of header information H and the content of the document is denoted as

M . To ensure security, Bob classifies the document as “confidential” and signs the document. The signature of the document is $Sig(D)$. Also, the content of the official document is encrypted by Alice’s private key. The encrypted content is denoted as $d_{Alice}(M)$. The sender (who can be either Bob or other staff at Bob’s agency who is responsible for sending all outgoing documents) then signs H , $Sig(D)$, and $d_{Alice}(M)$, encrypts H using Tom’s public key, and sends them to the official document exchange center. Once the document is received, Tom can only verify the document and decrypt the header information. The content of the document can not be read by Tom or anyone else. Alice is the only one who can verify the integrity and read the content of the document.

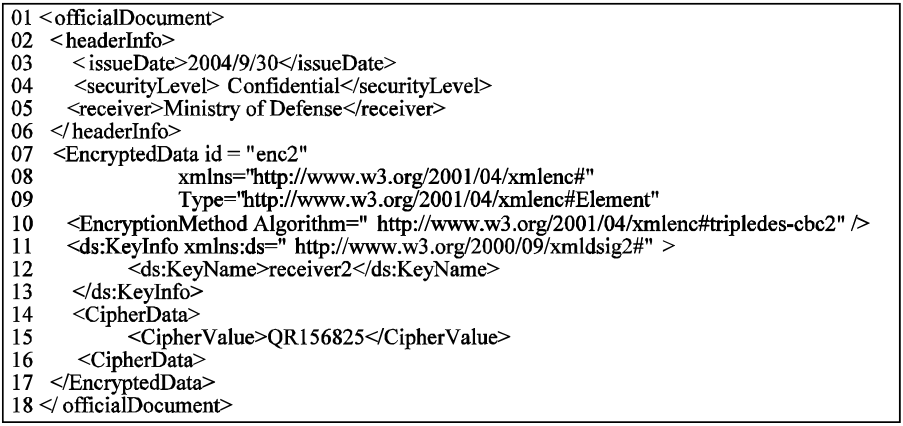
An example XML signature is shown in Figure 10. This signature is associated with an example ciphered document that is given in Figure 11 using the method of enveloping signature. As shown in Figure 11, the document was encrypted using two different public keys – *receiver*1 and *receiver*2. The header information was encrypted using *receiver1*’s public key and is shown in lines 2 to 12. And the content of the document was encrypted using *receiver*1’s public key and is shown in lines 13 to 23.

When *receiver*1 gets the ciphered document through the official document exchange center, s/he can use her/his private key to decrypt the ciphered document and obtain



```
01 <officialDocument>
02  <EncryptedData id = " enc1"
03                  xmlns = "http://www.w3.org/2001/04/xmlenc#"
04                  Type = "http://www.w3.org/2001/04/xmlenc#Element"
05    <EncryptionMethod Algorithm="  http://www.w3.org/2001/04/xmlenc#tripledes-cbc1" />
06    <ds:KeyInfo xmlns:ds="  http://www.w3.org/2000/09/xmldsig1#"  >
07          <ds:KeyName> receiver1 </ds:KeyName>
08    </ds:KeyInfo>
09    <CipherData>
10          <CipherValue>AB123567</CipherValue>
11     <CipherData>
12  </EncryptedData>
13  <EncryptedData id = "enc2"
14                 xmlns = "http://www.w3.org/2001/04/xmlenc#"
15                 Type = "http://www.w3.org/2001/04/xmlenc#Element"
16    <EncryptionMethod Algorithm="  http://www.w3.org/2001/04/xmlenc#tripledes-cbc2"/>
17    <ds:KeyInfo xmlns:ds="  http://www.w3.org/2000/09/xmldsig2#"  >
18          <ds:KeyName> receiver2 </ds:KeyName>
19    </ds:KeyInfo>
20    <CipherData>
21          <CipherValue>QR156825</CipherValue>
22     <CipherData>
23  </EncryptedData>
24</officialDocument>
```

Figure 11: The Encrypted Official Document.



```
01 <officialDocument>
02  <headerInfo>
03     <issueDate>2004/9/30</issueDate>
04     <securityLevel> Confidential</securityLevel>
05    <receiver>Ministry of Defense</receiver>
06  </headerInfo>
07   <EncryptedData id = "enc2"
08                    xmlns="http://www.w3.org/2001/04/xmlenc#"
09                    Type="http://www.w3.org/2001/04/xmlenc#Element"
10    <EncryptionMethod Algorithm=" http://www.w3.org/2001/04/xmlenc#tripledes-cbc2" />
11    <ds:KeyInfo xmlns:ds=" http://www.w3.org/2000/09/xmldsig2#" >
12            <ds:KeyName>receiver2</ds:KeyName>
13     </ds:KeyInfo>
14     <CipherData>
15            <CipherValue>QR156825</CipherValue>
16      <CipherData>
17  </EncryptedData>
18 </ officialDocument>
```

Figure 12: The Official Document Decrypted by *Receiver*1.

the header information of the document. The official document decrypted by *receiver*1 is shown in Figure 12. As can be seen from the figure, the content of the document in lines 7 to 17 is still invisible to *receiver*1.

Analysis

Since public-key certificates are used to authenticate both senders and recipients, digital signatures are used to ensure the integrity of the official documents, and the documents are encrypted using the RSA cryptosystem, the proposed model is secure. In the rest of this section, the proposed model will be analyzed in terms of fine-grained control and issues related to open standards and system integration.

- *Fine-grained control*: Although, in the past many official document exchange models were developed,[26,27,28,29] the signed and encrypted documents have to be a whole file or a document. According to these models, it is not possible to selectively sign and/or encrypt segments of a document when the security level of each segment of the document is different. Since the proposed model is extended from the standard drafts of XML Signature and XML Encryption, an originator or a sender can sign and encrypt selected portions of the document that he or she is responsible for, and then the designated recipient can decrypt and read the content of the document for which s/he has permission. It should be noted that the granularity is limited to the element level.

- *Conforms to XML Signature and XML Encryption*: The XML Signature and the XML Encryption are specification drafts currently under development jointly by the W3C XML Signature Working Group and the W3C XML Encryption Working Group. Both specification drafts describe a set of XML elements and attributes which are used to store information such as the signature itself, the encrypted data, and the algorithm used to generate signatures and ciphered data.[30,31] Although the standard can be applied to an arbitrary document, it is best suited for XML documents. Due to the fact that the proposed model is designed based on such standards, it conforms to the XML Signature and XML Encryption standards.
- *Compatible with the official document exchange model in Taiwan*: The architecture of the proposed model, as shown in Figure 7, is almost identical to the architecture of the official document exchange model in Taiwan, given in Figure 1. The only difference is the schemata of the exchanged official documents. Although the structure of the official documents in government agencies may be different, the proposed model already illustrated the kernel design of the signature and the ciphered documents. As a result, the design of signature or encrypted document can be slightly modified to meet the requirements of the different agencies.

Conclusions

XML has become a standard format for data interchange on the web, and it is widely adopted by the governments to exchange official documents. Therefore, the development of a secure fine-grained official document exchange model is extremely important. Since the traditional document exchange models lack granular control on official documents, security leaks are possible. This article—taking advantage of the rich structure of XML, XML Signature, and XML Encryption—proposes a secure fine-grained official document exchange model for e-Government. Due to the fact that the RSA cryptosystem is also adopted in the proposed model, it is secure. Also, since the proposed model enhances the current model used in Taiwan and follows the XML Signature and XML Encryption specification drafts, it can be easily incorporated into existing implementations.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC93-2213-E-018-014.

Notes:

[1] Chung-Huang Yang, Shy-Ming Ju, and T.R.N. Rao, "A Smartcard-Based Framework for Secure Document Exchange," in *Proceedings of IEEE 32nd Annual 1998 International Carnahan Conference on Security Technology* (Washington D.C., USA, 12-14 October 1998), 93-96, <citeseer.ist.psu.edu/yang98smartcardbased.html> (23 November 2004).

[2] International Council for Information Technology in Government Administration, "E-Government Development in Taiwan," *ICA Information* 82 (The Executive Yuan, Taiwan, June 2004) <http://www.ica-it.org/docs/issue82/issue_82_2004_06.html> (23 November 2004).

[3] IDA, "Secure Exchange Infrastructure for e-Government Presented in France," *eGovernment News* (6 October 2004), <http://europa.eu.int/ida/en/document/3357/194> (23 November 2004).

[4] Chii-Wen Wu, Hwai-Ling Shan, Wen-Cheng Wang, Dung-Ming Shieh, and Ming-Hsin Chang, "E-Government Electronic Certification Services in Taiwan," (paper presented at the Second International Workshop for Asia Public Key Infrastructure, IWAP 2002) (Taipei, Taiwan, 30 October-01 November 2002), <http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionC/25.pdf> (23 November 2004).

[5] *The Official Document Exchange System for e-Government in Taiwan*, <http://community.nat.gov.tw/> (23 November 2004).

[6] International Council for Information Technology in Government Administration, "E-Government Development in Taiwan."

[7] The Treasury Department of Taiwan, *Official Document Exchange Center for e-Government*, <http://210.241.98.149/ntact/index-1.htm> (23 November 2004).

[8] Charles F. Goldfarb and Paul Prescod, *The XML Handbook* (Englewood Cliffs: Prentice-Hall, 1998).

[9] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, and François Yergeau, eds., *Extensible Markup Language (XML) Version 1.0* (W3C, February 1998), <http://www.w3.org/TR/REC-xml/> (22 November 2004).

[10] Ronald L. Rivest, Adi Shamir, and Leonard Adleman, "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1978): 120-126, <http://theory.lcs.mit.edu/~rivest/publications.html> (22 November 2004).

[11] Elisa Bertino, Barbara Carminati, and Elena Ferrari, "XML Security," *Information Security Technical Report* 6, no. 2 (2001): 44-58.

[12] *XML Signature* (W3C XML Signature Working Group, 2001), <http://www.w3.org/Signature> (22 November 2004).

[13] *XML Encryption* (W3C XML Encryption Working Group, 2001), <http://www.w3.org/Encryption/2001> (22 November 2004).

[14] Yang, Ju, and Rao, "A Smartcard-Based Framework for Secure Document Exchange."

[15] Eric Jui-Lin Lu and Rai-Fu Chen, "An XML Multisignature Scheme," *Applied Mathematics and Computation* 149, no. 1 (February 2004): 1-14.

[16] Lu and Chen, "An XML Multisignature Scheme."

[17] *XML Signature* (W3C XML Signature Working Group, 2001).

[18] Donald Eastlake, Joseph Reagle, and David Solo, eds., *XML-Signature Syntax and Processing* (W3C Working Draft, 2000), <http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/> (22 November 2004).

[19] Bertino, Carminati, and Ferrari, "XML Security."

[20] Tzong-Chen Wu, Chih-Chan Huang, and D.-J. Guan, "Delegated Multisignature Scheme with Document Decomposition," *Journal of Systems and Software* 55, no. 3 (January 2001): 321-328.

[21] Bertino, Carminati, and Ferrari, "XML Security."

[22] Lu and Chen, "An XML Multisignature Scheme."

[23] *XML Encryption* (W3C XML Encryption Working Group, 2001).

[24] *XML Path Language (XPath) Version 1.0* (W3C, November 1999), <http://www.w3.org/TR/xpath> (22 November 2004).

[25] *XML Schema* (W3C, May 2001), < http://www.w3.org/XML/Schema.html> (22 November 2004).

[26] Chung-Huang Yang, So-Lin Yen, Hwang David Liu, Kuei Liu, Bor-Shenn Jeng, Kung-Yao Chang, Min-Shin Chang, Yu-Ling Cheng, Jo-Ling Liang, and Don-Min Shien "Secure Official Document Mail Systems for Office Automation," in *Proceedings of IEEE 31st Annual 1997 International Carnahan Conference on Security Technology* (Canberra, Australia, October 1997), 161-164.

[27] Shy-Ming Ju, "An SGML-Based Office Document Exchange and Management," in *Proceedings of SGML/XML Europe'98* (Paris, France, May 1998), 269-282.

[28] Yang, Ju, and Rao, "A Smartcard-Based Framework for Secure Document Exchange."

[29] *The Official Document Exchange System for e-Government in Taiwan*.

[30] Mark O'Neill, "XML and Security," *The XML Journal* 2, no. 12 (December 2001): 10-15.

[31] Bertino, Carminati, and Ferrari, "XML Security."

YI-HUI CHEN is currently a Ph.D. student at the Department of Computer Science and Information Engineering of the National Chung Chen University. She received her B.M. and M.S.I.M. degrees in Information Management from Chaoyang University of Technology, Taichung, Taiwan, in 1997 and 2004, respectively. Her research interests include XML, Access Control, Delegation, and Distributed System. *Address for correspondence:* Department of Computer Science and Information Engineering, National Chung Cheng University, 160 San-Hsing, Min-Hsiung, Chia-Yi, Taiwan, R.O.C.

ERIC JUI-LIN LU received his B.S. degree in Transportation Engineering and Management from the National Chiao Tung University, Taiwan, R.O.C., in 1982; a M.S. degree in Computer Information Systems from San Francisco State University, CA, USA, in 1990; and a Ph.D. degree in Computer Science from University of Missouri-Rolla, MO, USA, in 1996. In the period 1997-2004, he was a professor at the Department of Information Management and had served as Director of the Computer Center and Head of Graduate Institute of Networking and Communication Engineering at Chaoyang University of Technology, Taiwan, R.O.C. He is currently a professor at the department of Computer Science and Information Engineering at the National Changhua University of Education, Taiwan, R.O.C. His current research interests include electronic commerce, distributed processing, and security. *Address for correspondence:* Department of Computer Science and Information Engineering, National Changhua University of Education, No.1 Gin-Der Road, Changhua, Taiwan, R.O.C. *E-mail:* jlu@cc.ncue.edu.tw. *URL:* http://dns.csie.ncue.edu.tw/~jlu/.