Key Recovery Based on XML for B2B

JU-HAN KIM KI-YOUNG MOON
Active Security Research Team
Electronics and Telecommunications Research Institute (ETRI)
161, Ka-Jong Dong Yu-Sung Gu, DaeJeon, Republic of Korea
{juhankim, kymoon}@etri.re.kr

Abstract: ESES/XKRS(XML-bases Key-Recovery System), which will be introduced in this paper, is a subsystem of ESES(ETRI Secure E-commerce Service) that has been implemented to support security services such as authentication, integrity, confidentiality and key-recovery. ESES/XKRS is a key-recovery system for B2B electronic commerce and its recovery method is key-escrow. It has been designed and been implemented to be used in enterprise environment. All messages in ESES/XKRS are signed and encrypted with the form of XML using ESES/Signature and ESES/Cipher, respectively. One of the characteristics of this key-recovery system is that one enterprise can recover documents from external key-recovery system in other enterprise and also from owns.

Key-Words: Key-Recovery System, XML Encryption and XML Digital Signature

1. Introduction

In these several years, XML is one of languages that have been widely used and rapidly expanding, due to many advantages such as simplicity of learning, reading and using it, richness of data structure, portability and so on. And it is accepted as a standard in ebXML(electronic business Extensible Markup Language) for next generation electronic business. Nowadays XML security such as XML digital signature and XML encryption has been developed to represent legacy security to XML format at W3C.

The growth of this kind of security technologies provides a way that enables us to verify the existence and the confidence of each other on the Internet, and provides a means to keep confidentiality about communications.

The progress of security has brought the development of the means of telecommunications like the Internet and the expansion of all sorts of electronics business. However, there are some people begin to use those security technologies spreading widely at illegal things. That is, encryption technology of the security happened to be used illegally at conspiracy of crime and so on. It is caused by the fact that only one who has a right key can decrypt a cipher text.

In misuses of the technology, there are crime, terrorism and etc. on national aspect, and loss of key, hiding key intentionally and etc. on an individual or enterprise aspect. To solve the problem, Key-recovery comes out.

ESES/XKRS (XML-bases Key-Recovery System), which will be introduced in this paper, is a subsystem of ESES (ETRI Secure E-commerce Service) that

has been implemented to support security services such as authentication, integrity, confidentiality and key-recovery. ESES/XKRS is a key-recovery system for B2B electronic commerce and its method for recovery is key-escrow. It has been designed and been implemented to be used in enterprise environment. All messages in ESES/XKRS are signed and encrypted with the form of XML using ESES/Signature and ESES/Cipher that have been implemented in accord to specifications of XML Digital Signature group and XML Encryption group in W3C, respectively. One of the characteristics of this key-recovery system is that one enterprise can recover documents from external key-recovery system in other enterprise and also from owns.

2. The Structure of the system

In this section, the structure of ESES, ESES/XKRS and KRM (Key-Recovery Module) will be introduced.

2.1 ESES

As is mentioned above, ESES has ESES/Signature, ESES/Cipher and ESES/jcrypto as its subsystem. ESES/jcrypto provides cryptography library to the other subsystem. And ESES includes ESES/XKRS that provides key-recovery system. ESES/XKRI defines interfaces among ESES/ Signature, ESES/Cipher and ESES/XKRS and enables the structure of ESES to be more flexible. It also provides interfaces for modules in XKRS such as KRM, user module, manager module, and data repository.

The following Fig.1 shows the structure of ESES

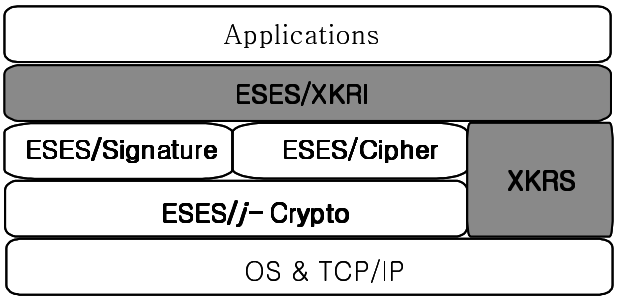

Fig.1 The structure of ESES

2.2 ESES/XKRS

Fig.2 on next page shows systems of two companies that have KRM, data repository module, and other modules and interfaces among them, XKRI, respectively. Each system in two companies is same one. Like a Fig.2, documents for key-recovery include documents generated in internal system of one company and documents generated in external system of it. In case of documents generated internal of one company, keys are saved at KRM of internal key-recovery server when documents are encrypted. In case of documents from external company, keys are stored when documents that have been encrypting are decrypted. Therefore, key-recovery for external documents in internal server performs a same way that key-recovery for internal document does.

For generating internal documents or decrypting external documents, XKRI stores keys that are used to encrypt or decrypt documents in key repository at KRM. It also saves encrypted documents at data repository. This enables a key-recovery system to recover all documents concerned with it.

Documents generated internally in one company are signed and encrypted using ESES/Signature and ESES/Cipher that have been implemented in accord to specifications of XML Signature group and XML

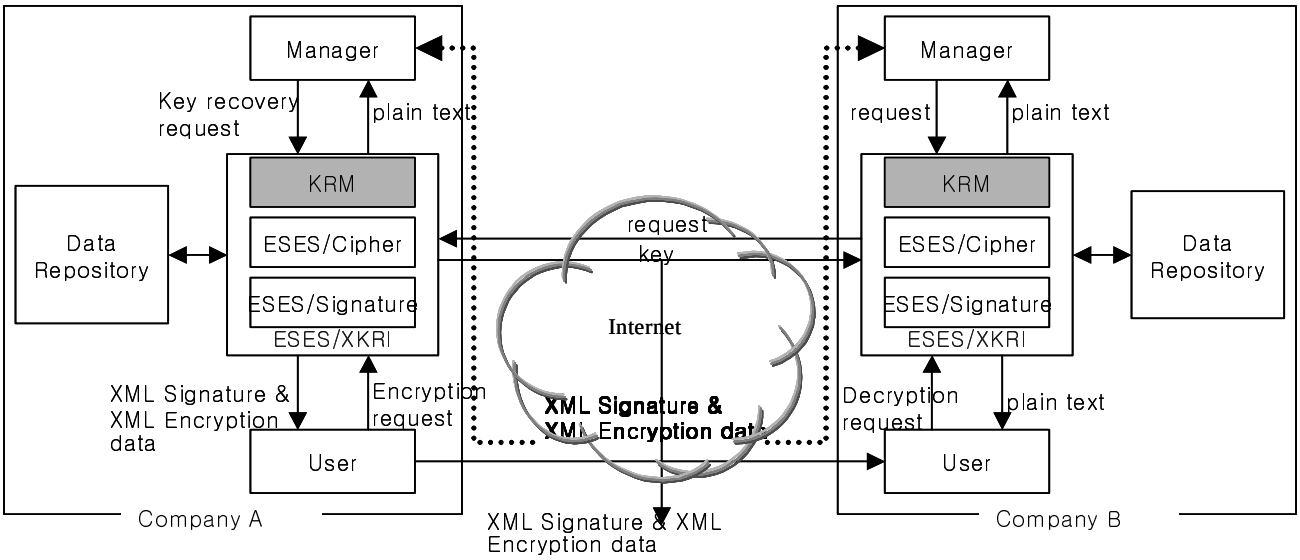

Fig. 2 Key-Recovery System

Encryption group in W3C.

Then the result documents are XML documents conforming to standards of W3C. Therefore, documents generated in external of one company and are coming inside should be XML documents consistent with the standard of XML Signature group and XML Encryption group.

2.3 KRM

KRM (Key-Recovery Module) has two public key pairs. One is used in only KRM and not opened to anybody. The other is used externally and updated periodically. One can use the public key of external public key pair by request to send an encrypted message to KRM.

Internal public key pair is to store a key to key repository in KRM and extract a key from key repository. When a key is stored in repository, it is encrypted with public key of internal key pair. And when it is extracted from repository, it is decrypted with private key of internal key pair.

Like a Fig 3, KRM consists of several sub modules. The key repository is used to save encrypted symmetric keys, the KRR (Key Recovery Requestor) repository to register persons who have a right to request key-recovery and the key manager module to execute all processes in KRM.

The key manager module decrypts the symmetric key encrypted with external public key of KRM by user module and encrypts it with internal private key. Then it stores the encrypted key in key repository.

When the key manager module receives the key from user module, it returns XMLKeyRecovery element that has some information about the key, person who has a right of key-recovery, KRM generating the key and so on, with the form of XML.

It also sends the manager module a key, when the manager that has already registered in KRR repository demands key-recovery. The key for the manager module is encrypted with the manager's public key.

The KRR repository is to register persons that have a right to request key-recovery. The key manager

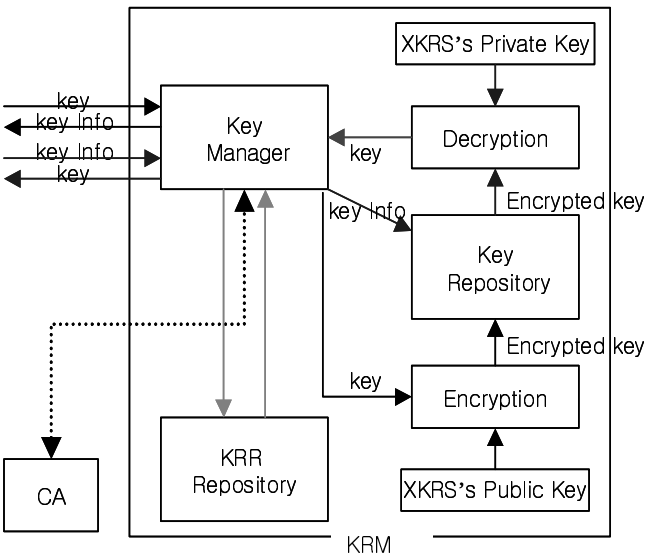

Fig.3 The structure of KRM

module always ignores a key-recovery request from one who is not registered in KRR repository.

3. The method of key-recovery

There are two methods for key-recovery in ESES/XKRS. One is to recover keys from internal system of a company and the other from key-recovery system of another company. This method is external key-recovery. The external key-recovery method needs communication between the KRM of a company and the other KRM of another company. The interface between two KRM is also defined in XKRI. If both companies use XKRI, key-recovery can be performed without intervention of any user or manager. It is possible to recover a key by only using XKRI for communication of both companies. However, when key-recovery policy needs manager's approval, KRM does not recover any key until getting it.

If the system requesting key-recovery is not using XKRS, it should make interface based upon it of the other's system. In other words, it should request key-recovery with correct data format with exact communication protocol of another system using XKRS.

The external key-recovery method, requesting to the system of another company, can be a part of backup system against internal system and protecting documents from attack with attention of making fabrication by users. Because it is possible to exchange documents between key-recovery systems, a manager can compare two documents from internal and external system. External systems can be backup systems for internal system. If internal system cannot operate normally by being attacked or any accident, it can recover documents related with other companies by requesting key-recovery. However, if there are some documents that are generated and used only inside, those documents cannot be recovered by external recovery.

Key-recovery system that is introduced in this paper will be used in B2B electronic commerce system and then there will be not so many such documents.

4. The Steps of Encrypting/Decrypting A Document

The Fig.4 on next page shows the steps of encrypting/decrypting a document and storing a key used in encrypting the document.

The procedure is as follows:

1. A request for encryption. Generate a symmetric key, K_AB.
2. XMLEnc $_{PK\_KRM\_A\_Ex}$(XMLDSig $_{PrK\_A}$(K_AB| Cert_A)).
3. Generate XMLKeyRecovery.

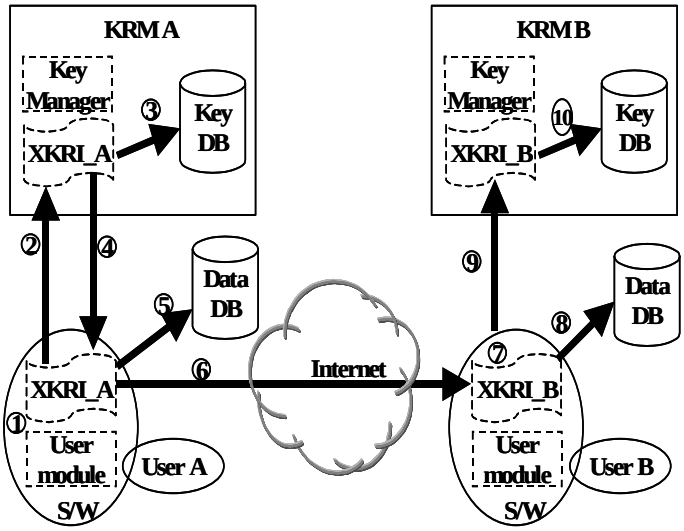

Fig. 4 Steps for Storing a Key

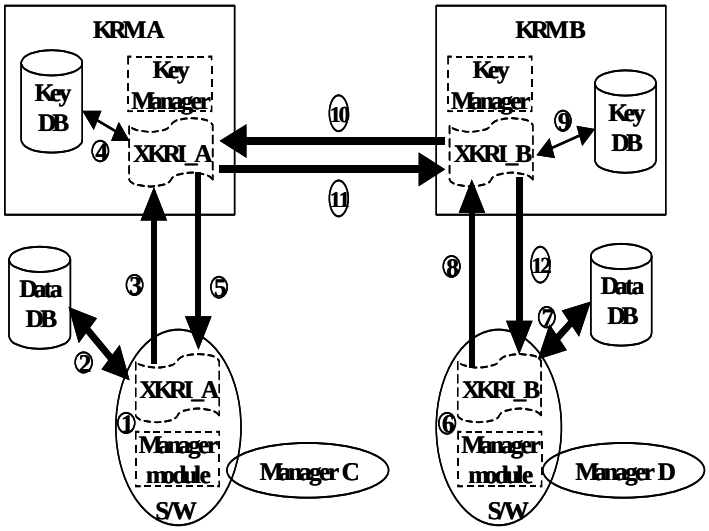

Fig. 5 Procedure of Key-Recovery

$XMLEnc_{PK\_KRM\_A\_In}$(K_AB) | XMLKeyRecovery

4. XMLEnc_enc $_{PK\_A\ K\_R}$(XMLKeyRecovery).
5. $XMLEnc_{PK\_B\ K\_AB}$($XMLSign_{PrK\_A}$(m)| XMLKey-Recovery).
6. $XMLEnc_{PK\_B\ K\_AB}$($XMLSign_{PrK\_A}$(m)| XMLKey-Recovery).
7. A request for decryption.
8. $XMLEnc_{PK\_B\ K\_AB}$($XMLSign_{PrK\_A}$(m)| XMLKey-Recovery).
9. XMLEnc $_{PK\_KRM\_B\_Ex\ \ K\_R}$(XMLDSig $_{PrK\_B}$(K_AB | XMLKeyRecovery)).
10. $XMLEnc_{PK\_KRM\_B\_In}$(K_AB) | XMLKeyRecovery.

Where $XMLDSig_{Prk}$(M) is XML form of Sig_{PrK}(M)| M | Cert, $XMLEnc_K$(M) is E_K(M), and XMLEnc $_{PK\ K}$(M) is E_K (M) | E_{PK} (K). K_R is a symmetric key generated randomly.

5. Procedure of Key-Recovery

The above Fig.5 shows the steps of key-recovery.

As is mentioned above, there are two methods for key-recovery. One is from internal system and the other from key-recovery system of another company.

In Fig.5, the process from step 1 to step 5 come under the internal key-recovery, the others the external key-recovery.

The procedure of the internal is as follows:

1. A request for document retrieval.
2. Document, $XMLEnc_{PK\_B\ K\_AB}$($XMLSign_{PrK\_A}$(m) | XMLKeyRecovery).
3. XMLEnc $_{PK\_KRM\_A\_EX\ \ K\_R}$ (XMLDSig $_{PrK\_C}$ (XMLEnc $_{PK\_B\ \ K\_AB}$ (XMLSign $_{PrK\_A}$ (m) | XMLKeyRecovery))|XMLKeyRecoveryRequest| Cert_Manager_C)
4. XMLEnc $_{PK\_KRM\_A\_In}$(K_AB).
5. XMLEnc $_{PK\_C\ K\_AC}$ (XMLDSig $_{PrK\_KRM\_A\_Ex}$ (m))

The procedure of the external is as follows:

6. A request for document retrieval.
7. Document, $XMLEnc_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$ (m) | XMLKeyRecovery).
8. XMLEnc $_{PK\_KRM\_B\_EX\ \ K\_R}$(XMLDSig $_{PrK\_D}$ (XMLEnc $_{PK\_D\ \ K\_AB}$(XMLSign $_{PrK\_A}$ (m) | XMLKeyRecovery))| XMLKeyRecoveryRequest | Cert_Manager_D).

9. XMLEnc $_{PK\_KRM\_B\_In}$(K_AB)

If there is not a request for the external key-recovery, go step 12. If there is, skip step9 and go step 10.

10. XMLEnc $_{PK\_KRM\_A\_EX\ K\_R}$(XMLDSig $_{PrK\_D}$ (XMLEnc $_{PK\_D\ K\_AB}$(XMLSign $_{PrK\_A}$ (m) | XMLKeyRecovery))| XMLKeyRecoveryRequest | Cert_Manager_D).
11. XMLEnc$_{PK_KRM_B_EX\ K_R}$(XMLDSig$_{PrK_KRM_A_Ex}$ (m)).
12. Generate a symmetric key, K_AC.

XMLEnc$_{PK_KRM_B_EX\ K_R}$(XMLDSig$_{PrK_KRM_A_Ex}$ (m)).

6. Conclusion

In this paper, we have designed ESES/XKRS that is a key-recovery system for B2B electronic commerce and its method for recovery is key-escrow. It has been designed and been implemented to be used in enterprise environment. All documents between companies are signed and encrypted with the form of XML using ESES/Signature and ESES/Cipher that have been implemented in accord to specifications of XML Digital Signature group and XML Encryption group in W3C, respectively.

There are two methods for key-recovery in ESES/XKRS. One is to recover keys from internal system of a company and the other from key-recovery system of another company.

The external key-recovery method, requesting to the system of another company, can be a part of backup system against internal system and protecting documents from attack with attention of making fabrication by users.

Finally, ESES including ESES/XKRS has been implemented with Java and its data structure is the XML. And it consists of APIs like a library. Therefore ESES is lightweight and it is easy to adapt ESES to lots of applications.

References

[1] Takeshi Imamura, Blair Dillaway and Ed Simon, “XML Encryption Syntax and Processing”, http:// www.w3.org/TR/xmlenc-core/, 2002

[2] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, “XML-Signature Syntax and Processing”, http:// www.w3.org/TR/xmldsig-core/, 2002

[3] Jae Seung Lee, Young Soo Kim, Joo Young Lee, Ju Han Kim, Kyung Bum Kim and Seung Won Sohn, “A Design of the XML Security Platform for Secure Electronic Commerce”, *WorkShop on Information Security Applications*, 2000, Seoul, Korea

[4] Joo-Young Lee, Ju-Han Kim and Chung-Chan Na, “A Design of the ESES/j-Crypto For Secure Electronic Commerce”, *Internet and Multimedia Systems and Applications*,2001, USA

[5] Dorothy E. Denning, Dennis K. Branstad, “A Taxonomy for Key Escrow Encryption System”, *ACM*, Vol. 39, No. 3, 1996