情報保護學會論文誌
第12券 第5號, 2002. 10

B2B를 위한 XML 기반의 키 복구 구현

김 주 한*, 문 기 영*, 손 승 원*

Implementation of Key Recovery Model based on XML for B2B

Ju-han Kim*, Ki-young Moon*, Sung-won Sohn*

요 약

이 논문에서는 B2B 시스템에서 사용할 수 있는 XML 기반의 키 복구 설계에 대해 소개한다. 이 키 복구는 시스템 내에서 사용되는 전자서명과 암호화를 W3C(World Wide Web Consortium)에서 최근 정의하고 있는 XML 전자서명(XML Digital Signature)과 XML 암호화(XML Encryption)를 사용한다.

서명이나 암호화한 결과 값이 XML 문서 형태로 구성되고 시스템 전반에 사용되는 메시지들이 또한 모두 XML 문서 형태로 구성됨으로 기존의 XML 응용 및 XML 기반의 전자상거래 플랫폼에 투명하게 접목이 가능하다. 또한, 키 복구 방식으로는 키 위탁방식을 사용하며 기업에서 사용할 수 있도록 설계되고 구현되었다. 이 키 복구는 회사 내의 키 복구 서버로부터의 키 복구는 물론, 거래가 있는 다른 회사의 키 복구 서버에 대해 그 거래에 해당하는 문서의 키 복구 요청도 가능한 것이 그 특징이다.

ABSTRACT

In this paper, we will introduce a design of key recovery based on XML can be used in B2B environment. XML Digital Signature and XML Encryption that are defined recently as standards by W3C(World Wide Web Consortium) are deployed to sign/verify or encrypt/decrypt documents for electronic commerce and keys to store/load at/from key recovery server.

The result of signature or encryption is always an XML document and all messages used in this key recovery system are also XML documents. It enables to adapt transparently this key recovery system to legacy XML applications and electronic commerce platforms based on XML. And its method for key recovery is key escrow. One of the characteristics of this key recovery is that one enterprise can recover keys of some documents for electronic commerce from external key recovery system in other enterprises related with them and also recover keys from owns.

Keyword : *Key Recovery, XML Digital Signature, XML Encryption, B2B*

Ⅰ. 서 론

키 복구 시스템이란 집행기관이 범죄 수사를 목적으로 암호문을 복호해야 한다거나, 암호문의 소유자가 암호문에 사용된 키를 분실해서 중요 데이터를 복호할 수 없을 경우 등에 한해 허가된 사람에게 해당하는 암호문에 한해서 복호화가 가능한 능력을 제공하는 암호 시스템이다. 허가된 사람이란 시스템이 사용되기 전에 미리 합의되어 복구 능력을 가질 수 있는 사람을 뜻한다. 이것은 정부기관, 개인, 기업 등이 될 수 있다. 즉, 키 복구란 암호 시스템에서 키를 가지고 암호문을 복호하는 정상적인 절차 외에 다른 방법으로 유사시에 암호문을 복호할 수 있는 방법이다. 복구 능력을 가진다는 것은 실제 데이터

* 한국전자통신연구원 네트워크보안연구부(juhankim@etri.re.kr, kymoon@etri.re.kr, swsohn@etri.re.kr)

를 암호화한 키 자체를 얻어내거나 또는 복호된 평문을 얻는 것을 말한다. 암호문 생성 시에 암호알고리즘 외에 어떤 특정한 메커니즘을 통해서 이러한 방식을 지원하는 것이 가능하다.

키 복구가 초기에는 법 집행기관의 범죄 수사를 목적으로 제안되었다. 그러나 기업이나 민간인들의 반발에 의해서 정책이나 요구사항이 많이 변경되었고, 현재에는 전자 상거래와 같은 상업적 목적에 주로 사용된다.

이 논문에서 소개되는 키 복구 모델은 XML을 기반으로 한다. XML은 문서에 대한 세계적인 표준이며 또한, 한 문서의 논리적 구조를 표현하고 데이터를 정의, 포함하고 있는 태그를 생성함으로써 데이터 교환 등에서도 표준으로 자리잡고 있다. XML 태그는 데이터를 받은 프로그램에게 어떻게 읽을 것인지에 대한 정보를 제공한다. 한 XML 문서는 DTD (document type definition) 혹은 스키마(schema)에 의해 설명되기 때문에, 이 문서를 전에 한번도 받아본 적이 없던 프로그램도 기대되는 데이터가 어떤 것인지 그리고 데이터가 완성된 것인지 아닌지를 판단할 수 있다. 그리고, XML은 관계형 데이터베이스 등의 공통적인 오버헤드를 감소시켜 주며 제품과 플랫폼에 상관없이 다중 테이블들을 위한 복합적인 스키마를 생성함으로써 데이터가 데이터베이스 등에 XML 형태로 직접 저장되게 되는 장점을 갖는다.

XML 기반의 키 복구 모델은 내부에 사용되는 메시지뿐만 아니라, 키 복구 시스템의 기반이 되는 암호/복호 및 서명/검증에서도 XML이 기반이 되는 전자서명과 암호화를 사용하며, 각기 W3C(World Wide Web Consortium)에서 최근 정의하고 있는 XML 전자서명[1] (XML Digital Signature)과 XML 암호화[2] (XML Encryption)의 기술문서들을 구현한 것을 사용하여 키 복구 모델을 구성한다. 암복호 및 서명에 XML 보안 표준을 사용함으로써 기존의 XML 응용 및 XML 기반의 전자상거래 플랫폼에 투명하게 접목이 가능하다. 기존의 제품 및 전자상거래 플랫폼에 세계적인 표준을 적용하는 함으로써 기존의 상거래 시에 발생할 수 있는 데이터 통합 작업을 상당히 감소시키는 효과를 갖는다. 그리고, 암복호 및 서명 체계가 하나로 통합되어 사용됨으로써 서로 기업 간의 전자상거래(B2B)에 필요한 사전 준비 작업도 아주 간소해지는 장점을 생긴다.

키 복구는 방식에 따라 키를 위탁하는 키 위탁 방식[3~5]과 키 캡슐화 방식이 있다. 키 위탁 방식은 사용자의 키 전부 혹은 일부분씩 나누어서 믿을 수 있는 기관 혹은 기관들에 분산 배치하는 방식이다. 키 캡슐화 방식은 키 복구 필드 또는 데이터 복구 필드라는 키 복구에 필요한 정보들을 메시지의 암호화 전송 때 같이 붙여서 보내거나 파일을 암호화 저장할 때 같이 저장하여 키 복구가 가능하게 하는 방식이다.

키 위탁 방식에서 키의 종류에 따라 개인키처럼 긴 주기의 키(long-term)를 저장하는 방식이 있고, 세션키처럼 자주 변경되어 사용되는 짧은 주기의 키(short-term key)를 저장하는 방식으로 나눌 수 있다.

본 논문에서 소개하는 키 복구 모델은 세션키를 저장하는 키위탁 방식을 사용하며 회사 내의 키 복구 서버로부터의 키 복구는 물론, 거래가 있는 다른 회사의 키 복구 서버에 대해 해당하는 거래의 문서에 대해 키 복구 요청도 가능한 것이 특징이다. 내부의 키 복구 시스템이 악의적인 공격이나 기타 사고에 의해 사용할 수 없을 시에, 외부 키 복구 시스템을 사용하여 키 복구를 할 수 있다. 또한, 상대회사 사용자가 보내온 문서를 확인하기 위해, 상대의 키 복구 서버에 받은 문서를 보내면, 상대 회사의 키 복구 서버는 데이터 저장소에 저장되어 있는 문서와 비교를 하여 그 결과를 넘겨줌으로써 사용자 단계에서의 문서 조작을 막을 수 있는 특징이 있다.

다음 장에서는 키 복구 모델이 제시되고, 3장에서는 이 키 복구 모델이 가지고 있는 두 가지 키 복구 방법들을 설명한다. 그리고 4장에서는 키 저장 절차와 회사 내부에서의 키 복구 절차 및 외부 키 복구 절차 등이 제시된다.

II. XML 기반 키 복구 모델

이 장에서는 XML 기반 키 복구 모델의 특징, 키 복구 시스템의 구성 및 운영, 그리고 키 복구 모듈에 대해 차례로 소개한다.

2.1 특징

본 논문에서 제시하고 키 복구는 B2B 환경에서 적용하기 위한 것이다. B2B 환경 하에서는 B2B 데이터 표준 및 차세대 전자상거래의 표준으로 정착되고 있는 XML의 적용이 필요하다. 따라서, 본 논문에서는 거래 시에 상대 회사에 전송되는 데이터,

키 저장소에 저장되는 키 그리고 각종 모듈 등에서 문서 혹은 키의 암호화에 암호화/복호화, 서명/검증 시에 국제 표준인 XML 전자서명과 XML 암호화를 함께 적용하여 데이터 기밀성 및 무결성 그리고 인증 등을 제공한다. 키의 복구 요청 및 키 복구 결과 전송도 XML로 따로 구성하여 키 복구 시스템 전반에 걸쳐 XML을 사용하였다.

XML을 사용하여 키를 복구하는 기능은 W3C에서 정의하고 XKMS[6] (XML Key Management System)에도 있다. XKMS는 XML 처리가 수행되는 클라이언트 플랫폼 상에서 복잡하거나 전문화된 end-entity PKI 어플리케이션 로직을 대신하여 XML 기반 시스템이 신뢰관계를 구축하는데 그 목적이 있으며 이는 PKI 기반의 복잡성으로부터 벗어나 XML 클라이언트의 구현을 용이하게 한다.

XKMS는 긴 주기동안 사용하는 공개키 쌍을 사용하며, 믿을만한 제 3자에게 등록하는 것이 특징이다. 그러나, B2B 환경에서는 수많은 회사들과 많은 거래들을 하게 됨에 따라 그 거래들에 필요한 문서들을 사용자 별로 할당하는 공개키 쌍만으로 관리하기에는 부적절하다.

본 논문에서 제시하고 있는 B2B를 위한 XML 기반의 키 복구는 B2B 환경 하에서 적용하기 위해 각각의 회사들간의 매 거래 시마다 키를 달리 사용하는 세션키를 저장하여 암호 문서관리 및 복구에 보다 유용하다.

암호화에 사용되는 각 세션키의 저장은 믿을 만한 제 3자에게 키를 위탁하는 XKMS와는 달리, 각 회사별로 각기 키 복구 서버를 두어 저장하게 함으로써 키 복구 시스템을 쉽게 설치하고 사용할 수 있다. 그리고, 세션키를 사용함으로써 하나의 키가 노출된다 하더라도 그 키에 해당하는 문서가 제한적이기 때문에 긴 주기의 키를 사용할 때보다 안전하다.

또한, 이 키 복구 모델은 회사 내부에서 만들어서 외부로 가는 문서들 및 외부에서 들어온 문서들에 관련된 세션키들을 키 위탁방식으로 저장하게 된다. 한 회사를 중심으로 내부 및 외부 문서에 대한 세션키를 모두 저장하게 됨으로써, 다른 회사의 키 복구 서버로의 키 복구 요청도 가능한 것도 본 논문에서 제시하고 있는 키 복구의 큰 특징이다. 이는 다른 회사의 키 복구 서버들이 한 회사의 키 복구 시스템의 백업 역할을 할 뿐만 아니라, 사용자 단계에서의 거래 문서 조작 등의 악의적인 공격을 막을 수 있는 장점으로 작용한다.

본 논문에서 제시하는 키 복구 모델의 또 다른 특징은 상업적으로 사용되는 것에 중점을 두었으며 민간의 키 복구 요구 사항에 대해서는 고려하지 않았다. B2B의 특성상 거래에 해당하는 문서만 저장하게 됨으로써, 민간 요구 사항인 개인 정보 침해 사항에 대해서는 해당사항이 없기 때문이다. 정부기관에서의 키 복구 요청도 고려하지 않았다.

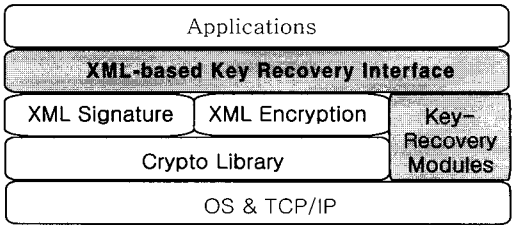
2.2 구조

〔그림 1〕은 XML 보안에 관련된 서브 시스템, 키 복구 모듈들이 있는 서브 시스템, 그리고 어플리케이션에서 이 서브 시스템들을 사용하기 위해 제공하는 인터페이스 서브 시스템을 보여준다.

B2B를 위한 키 복구 모델은 위와 같이 암호 라이브러리와 그를 기반으로 한 XML 전자서명과 XML 암호화가 서브 시스템을 구성한다. 또한, 실제적인 키 복구 시스템 구성을 위해 필요한 데이터 저장소, 사용자 및 관리자 모듈, 및 키 복구 모듈 등으로 구성된 키 복구 모듈 등이 키 복구 서브 시스템으로 구성된다. 이 서브 시스템들 위로 응용 프로그램과의 인터페이스를 제공하는 XML 기반 키 복구 인터페이스 서브시스템이 존재한다. 이 인터페이스 서브시스템은 XML 전자서명, XML 암호화, 키 복구 모듈들 및 암호 라이브러리 등의 각각의 서브 시스템들에 대한 구성의 융통성을 제공한다.

각각의 서브시스템들은 응용 프로그램에서 직접 호출할 수 없으며 인터페이스를 통해서만 가능하다. 인터페이스를 통하지 않고 직접 호출이 가능하게 되면, 암호 문서를 만드는 사용자가 임의로 암호화나 서명이 가능하게 되어 문서가 조작될 가능성이 있기 때문이다.

위에서 언급한 바와 같이, XML 전자서명과 XML 암호화는 W3C의 XML 전자서명 그룹과 XML 암호화 그룹에서 각기 정의하고 있는 표준을 따른다.



〔그림 1〕 XML 기반 키 복구 구조

이렇게 함으로써 내부적으로 암호화해서 데이터 저장소에 저장되는 문서나 그 문서에 대한 키를 저장하는 키 저장소에 대해 보다 편리하고 안전하게 문서나 키를 저장할 수 있다. 또한, 인터넷을 통한 문서의 교환에도 표준을 따르므로 별도의 데이터 통합 작업등이 필요하지 않게 된다.

2.3 운영

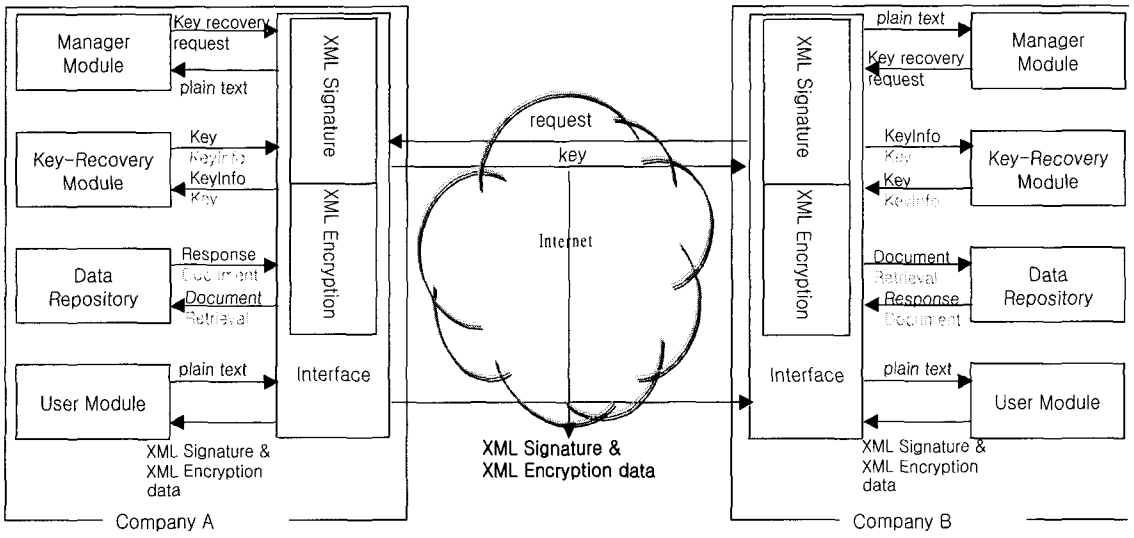
〔그림 2〕는 키 복구 모듈, 데이터 저장소, 사용자 및 관리자 모듈 그리고 그 것들 간의 인터페이스 등이 각각 있는 두 기업의 키 복구 시스템들의 운영을 보여주고 있다. 두 기업의 시스템은 모두 동일한 시스템이다.

〔그림 2〕에서처럼 모든 모듈간의 인터페이스는 논리적으로 한곳에서 관리되고 있으며, 다른 회사와의 인터페이스도 역시 같은 곳에서 관리한다. 그러나, 이 인터페이스들은 물리적으로 모든 모듈에 대해 같은 기능을 하지 않으며 각각의 모듈별로 기능별로 분리된 세부 인터페이스들을 조합하여 사용한다. 예를 들어, 사용자 모듈의 인터페이스에는 XML 전자서명 기능, XML 암호화 기능, 키 생성 기능, 키 복구 모듈에게 생성한 키를 전달하는 기능, 키 복구 모듈로부터 키 정보를 담은 KeyRecoveryInfo 엘리먼트(XML 문서의 한 노드)를 받는 기능, 서명되고 암호화된 결과에 위에서 생성된 엘리먼트를 붙여 최종 암호문을 만드는 기능, 데이터 저장소에 생성된 암호문을 저장하는 기능 등이 포함된다.

데이터 저장소의 인터페이스는 검색 요청에 따른 문서 반환 기능과 문서에 대한 저장 기능 등이 포함된다. 그리고, 키 복구 모듈은 키를 받아 키 정보를 생성하는 기능과 키 정보를 받아 키 복구를 하는 기능이 있다. 관리자 모듈은 문서를 검색 요청하는 기능, 받은 문서에 대한 키 복구 요청 기능 및 복호화된 문서를 표시하는 기능 등을 갖는 인터페이스들이 있다. 이들 세분화되어 있는 인터페이스들은 각각의 모듈에 조합되어 같이 포함되어 있다.

키 복구 대상 문서는 한 회사 내부에서 생성하고 내부에서 사용하는 문서, 내부에서 생성해서 외부 즉, 다른 회사로 보내는 문서 ,그리고 외부에서 생성되어 내부로 들어오는 문서로 나뉜다.

내부에서 생성 시에는 XML 암호화 시에 키가 키 복구 모듈에 저장된다. 외부에서 생성된 문서는 복호화 시에 키가 저장되므로, 내부와 외부의 문서에 상관없이 특정 암호문에 관련된 키가 키 복구 모듈에 저장된다. 따라서 한 키 복구 모듈은 내부에서 생성되거나 혹은 외부에서 생성되어 내부로 들어온 문서에 대해서도 모든 키를 저장하고 있게 된다. 물론, 데이터 저장소에는 위의 암호문이 모두 별도로 저장된다. 따라서, 외부에 키 복구 요청을 하지 않아도 자신과 관련된 모든 문서에 대한 키 복구가 가능하다. 물론, 상대 회사도 마찬가지로 자체 내의 문서와 상대 회사에서 생성해서 보낸 문서들을 모두 가지고 있다.



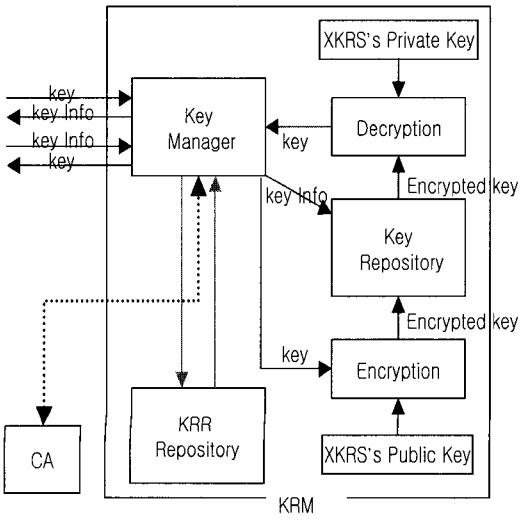
〔그림 2〕 시스템 운영도

키 복구되는 지역에 따라 내부 키 복구와 외부 키 복구로 나눌 수 있다. 내부 키 복구는 위에서처럼 한 기업의 내부에 있는 키 복구 모듈을 통해 키 복구를 하는 것이고 외부 키 복구는 다른 기업에 속한 키 복구 모듈에게 키 복구를 요청하는 것이다.

2.4 키 복구 모듈(Key Recovery Module)

〔그림 3〕처럼 키 복구 모듈(KRM: Key Recovery Module)은 여러 가지 서브 모듈들로 구성된다. 키 복구 모듈 외부와의 인터페이스 및 키 복구 모듈 안에서 키 저장 및 키 복구 프로세싱을 담당하는 키 관리 모듈, 미리 지정된 키 복구 권한자들을 등록하기 위한 KRR 저장소(KRR: Key Recovery Requestor) 및 키를 저장하는 키 저장소 등으로 구성되어 있다.

KRM은 두개의 공개키 쌍을 가지고 있다. 하나는 내부적으로 사용되며 전혀 공개되는 공개키 쌍이며, 다른 하나는 외부적으로 사용되며 주기적으로 갱신되는 공개키 쌍이다. 내부 공개키 쌍의 공개키는 키를 키 저장소에 저장할 때 암호화하여 저장하기 위해 사용된다. 또한, 내부 공개키 쌍 중 개인키는 키 복구 시 키 저장소에 암호화되어 있는 키를 복호화하기 위해 사용된다. 외부 공개키 쌍은 기타 모듈, 즉 사용자 모듈, 관리자 모듈 혹은 외부의 키 복구 모듈에서 데이터를 암호화 전송하기 위해 공개키를 요청할 때 주기 위한 것이다. 외부 공개키 쌍의 개인키는 다른 모듈에서 암호화해 전송한 데이터를 복호화할 때 사용한다.



〔그림 3〕 키 복구 모듈 구성도

두 개의 공개키 쌍은 키 복구 모듈의 서브 모듈인 키 관리 모듈에 의해 관리된다. 키 관리 모듈은 사용자가 외부 공개키 쌍의 공개키로 암호화해서 보내온 키를 복호화한다. 이를 다시 내부 공개키 쌍의 공개키를 이용 암호화하여 키 저장소에 저장하고, 그 키에 대한 키 정보를 담은 엘리먼트를 생성하여 사용자에게 반환하는 역할을 한다.

또한, 키 관리 모듈은 관리자가 키 복구 요구 시, 관리자의 인증서 검증을 하며, 정당한 키 복구 요청자라면 관리자가 보내온 암호 문서를 복호화하기 위해 필요한 키를 키 저장소에서 가져와 내부 개인키로 복호화한다. 이렇게 얻어진 키로 암호 문서를 복호화하여 얻은 평문을 다시 임의의 키를 생성하여 암호화한다. 그리고, 그 키를 관리자의 공개키로 암호화해서 보낸다. 키 저장소에서 복구된 키를 직접 암호화해서 보내지 않고 문서를 임의의 키로 다시 암호화하고 관리자의 공개키로 암호화해서 보내는 이유는 데이터 저장소의 문서들의 암호화된 형태가 항상 같기 때문에 암호화에 사용된 키가 일단 노출되면, 혹시라도 같은 키로 암호화된 문서들이 있을 시에 이 내용까지 노출된다. 따라서, 이를 막기 위해 키 저장소에 키를 직접 복호화해서 주지 않고, 요청한 문서를 복호화해서 주는 것이다.

키 관리 모듈은 위에서 언급한 두 가지 일, 키를 받아 키 정보 엘리먼트를 반환하고 그리고 키 정보를 받아 키를 반환하는 것, 이 외에 다른 키 복구 모듈이 보낸 문서에 대해 내부 데이터 저장소에 저장되어 있는 문서와 비교를 하고 그 결과를 반환하는 일도 한다.

KRR 저장소는 키 복구 권한자에 대한 정보를 저장하는 저장소이다. 여기에 등록되어 있는 사람에게만 키 복구를 한다. 내부에서 생성된 문서는 관리자 혹은 그 문서를 생성한 사람이 될 수 있다. 외부 문서의 경우에는 관리자 및 그 문서를 처리하는 사용자 이외에도 문서 교환 전에 등록시킨 상대방의 키 복구 권한자도 될 수 있다.

Ⅲ. XML 기반 키 복구 수행 방법

위에서 언급한 것처럼, 본 논문에서 제시하는 키 복구 방법은 내부 키 복구 방법과 외부 키 복구 방법 두 가지로 나눌 수 있다.

우선 자체 키 복구 모듈로 키 복구를 하는 방식과 상대 회사에게 키 복구 요청을 하는 방식으로 나눌

수 있다. 상대 회사에 키 복구 요청을 하는 방법은 자체의 키 복구 모듈과 상대 회사의 키 복구 모듈과의 통신을 통하여 이루어진다. 두 회사간의 통신에 관한 인터페이스도 역시 인터페이스 서브 시스템에 안에 정의되어 있다. 두 회사가 동시에 본 논문에서 제시하고 있는 키 복구 모듈을 사용한다면 키 복구에 대해 사용자의 개입이 이루어지지 않게 할 수도 있으며, 단순히 두 시스템의 인터페이스 사이의 통신만으로 키 복구를 할 수 있다. 그러나, 상대 키 복구 모듈의 키 복구 요청을 관리자의 허가가 있을 시에만 할 수 있도록 정책을 조정하는 것도 가능하다. 요청하는 쪽이 다른 시스템을 사용하고 있다면, 키 복구 요청자는 키 복구를 요청하는 시스템의 인터페이스를 따라 키 복구 요청을 해야 한다. 즉, 정확한 주소와 포트를 통해 키 복구를 요청해야 하며 정해진 XML 형태를 따라야 한다. 또한, 키 복구 프로토콜도 맞춰줘야 키 복구 모듈간의 키 복구가 가능하다.

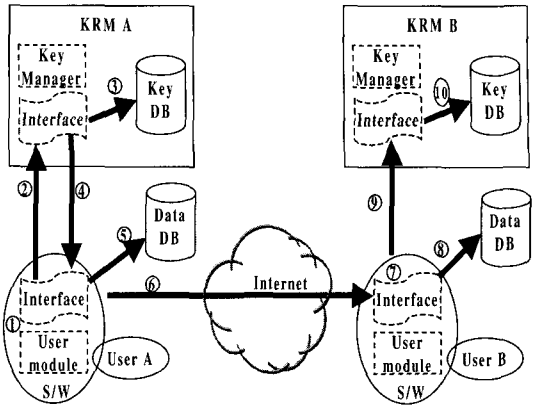
이러한 상대 회사에 키 복구 요청을 하는 방식은 문서 및 키 복구 시스템의 백업의 역할뿐만 아니라, 사용자 등의 악의적인 공격에서도 문서를 보호할 수 있는 역할도 하게 된다. 사용자들간에 주고받는 문서를 키 복구 서버간에 비교를 할 수 있으므로 사용자가 키 복구 방식을 사용하지 않고 임의로 서명/암호화하는 문서 조작을 막을 수 있게 된다.

백업의 역할이란 한 회사가 자체 키 복구 시스템을 악의적인 공격이나 기타 사고에 의해 사용할 수 없을 경우, 상대 회사의 키 복구 모듈에게 자신에게 해당된 문서들에 대한 키 복구 요청을 하게 된다. 키 복구 요청을 받은 회사는 자신이 요청한 회사에 보낸 문서나 상대에게 받은 문서 모두를 키 복구를 하여 요청회사에게 보낼 수 있다. 그러나, 자신의 회사 내에서 생성하여 오직 회사 내에서만 사용된 문서라면 외부 키 복구 방식으로는 키 복구 할 수 없게 되고 자체 키 복구 방식으로만 키 복구가 된다. 하지만, 본 논문에 기술되는 키 복구 시스템은 B2B 전자상거래를 위한 것이므로 자체적으로 생성하고 내부에서만 사용되는 암호문서는 많지 않을 것이다.

Ⅳ. 키 복구 수행 절차

4.1 암호문 생성 및 키 저장 절차

〔그림 4〕는 문서를 암호화하고 복호화하는 절차를 보여준다. 또한, 문서를 암호화하는데 사용된 키를 저장하는 절차를 보여준다.



〔그림 4〕 암호문 생성 및 키 저장 절차

키의 저장은 암호문을 생성할 때는 암호화 단계에서 저장되며, 그렇지 않을 때는 암호문을 받아 복호화할 때에 저장된다.

암호문 생성 및 키 저장 절차는 다음과 같다.

1. 암호화 요구.
   대칭키 K_AB 생성.
2. XMLEnc $_{PK\_KRM\_A\_Ex}$(XMLDsig $_{PrK\_A}$(K_AB | Cert_A)).
3. XMLKeyRecovery 엘리먼트 생성.
   XMLEnc $_{PK\_KRM\_A\_In}$(K_AB) | XMLKeyRecovery
4. XMLEnc $_{PK\_A\ K\_R}$(XMLKeyRecovery).
5. XMLEnc $_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$(m) | XMLKeyRecovery).
6. XMLEnc $_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$(m) | XMLKeyRecovery).
7. 복호화 요구.
8. XMLEnc $_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$(m) | XMLKeyRecovery).
9. XMLEnc $_{PK\_KRM\_B\_Ex\ K\_R}$(XMLDSig $_{PrK\_B}$(K_AB | XMLKeyRecovery)).
10. XMLEnc $_{PK\_KRM\_B\_In}$(K_AB) | XMLKeyRecovery.

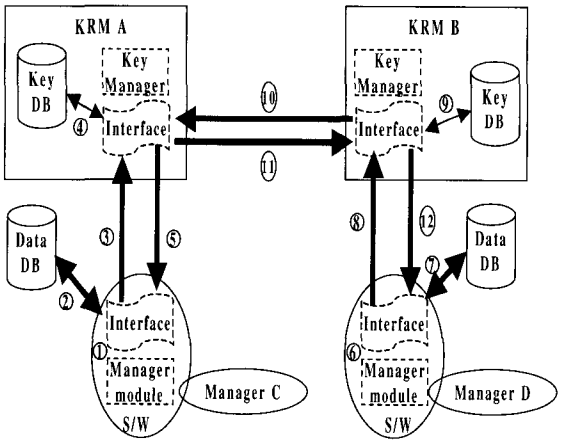
위에서 XMLDSig $_{Prk}$(M)은 Sig $_{PrK}$(M)|M|Cert를 XML 전자서명으로, XMLEnc $_{K}$(M)은 E_K(M)의 그리고 XMLEnc $_{PK\ K}$(M) 은 E_K(M) | E_{PK}(K)의 XML 암호화로 나타낸 것이다. K_R은

임의로 생성된 대칭키를, K_AB는 사용자 A와 B 사이에 사용되는 대칭키를, PK_KRM_A_In 및 PrK_KRM_A_In는 키 복구 모듈 A의 내부 공개키 쌍 중 각각 공개키와 개인키를 나타낸다. 또한 PK_KRM_A_Ex 및 PrK_ KRM_A_Ex는 외부 공개키 쌍의 공개키와 개인키를 의미한다.

4.2 키 복구 절차

위에서 언급한 바와 같이, 키 복구는 내부 키 복구 모듈을 이용하는 방법과 외부 키 복구 모듈을 이용하는 방법이 있다.

〔그림 5〕는 키 복구 절차를 나타낸다. 1~5단계는 내부 키 복구 모듈을 이용하는 방법을, 나머지 절차는 외부 키 복구 모듈을 이용한다.



〔그림 5〕 내부 및 외부 키 복구 절차

다음은 내부 키 복구 모듈을 사용하는 절차이다.

1. 문서 검색.
2. 문서, 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))

다음은 내부 및 외부 키 복구 모듈을 사용하는 절차이다.

6. 문서 검색.
7. 문서, XMLEnc $_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$(m) | XMLKeyRecovery).
8. XMLEnc $_{PK\_KRM\_B\_EX\ K\_R}$(XMLDSig $_{PrK\_D}$ (XMLEnc $_{PK\_B\ K\_AB}$(XMLSign $_{PrK\_A}$(m) | XMLKeyRecovery)) | XMLKeyRecoveryRequest | Cert_Manager_D).
9. XMLEnc $_{PK\_KRM\_B\_In}$(K_AB)
   외부 키 복구가 요청되지 않았다면, 12단계로 넘어간다. 요청되었다면, 9단계를 생략하고 10단계로 간다.
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. 대칭키 K_AC를 생성한다.
    XMLEnc $_{PK\_KRM\_B\_EX\ K\_R}$(XMLDSig $_{PrK\_KRM\_A\_Ex}$ (m)).

위 절차의 단계 10과 11은 다른 형태로도 운영이 된다. 위 절차에서는 10단계에서 키 복구하려는 문서에 키 복구 요청 문서와 인증서 등을 서명하고 암호화해서 보내고 11단계에서 키 복구가 된 문서를 임의의 대칭키로 암호화하고 그 키를 다시 요청한 사람의 공개키로 암호화해서 보낸다. 하지만, 10단계에서 키 복구 요청대신에 문서 확인 요청을 보내게 되면, 11 단계에선 받은 문서를 복호화해서 우선 키 복구 정보를 확인하고, 또한 자신의 데이터 저장소에 있는 문서와 비교하여 그 결과만을 반환한다. 이렇게 함으로써 임의의 사용자가 다른 서명, 암호 시스템을 사용하여 악의적으로 문서를 조작할 수 없게 된다.

〔그림 5〕에서 관리자 모듈은 키 복구 모듈에 접속할 때마다 키 복구 모듈로부터 새로 저장된 키에 대한 키 정보들을 담은 KeyRecoveryInfo 엘리먼트들만을 따로 받아 로컬 시스템 혹은 별도의 장소에 저장하게 된다. 이 엘리먼트들이 키 복구 모듈의 백업 역할을 한다. 다시 말해, 키 복구 모듈 정보, 송신자 및 수신자의 정보를 담고 있는 키 복구 정보 엘리먼트들은 키 복구 모듈과 데이터 저장소 모두가

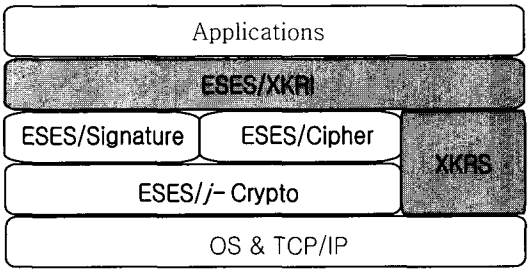
악의적인 공격이나 기타의 사유로 키 복구를 할 수 없을 경우를 위해 키 복구 모듈 이외에 장소에 별도로 저장되며, 이 키 복구 정보로 외부 키 복구 모듈에 키 복구를 요청할 수 있다.

V. 구 현

본 논문에서 소개된 키 복구 모델 및 XML 전자서명 및 XML 암호화 등은 ESES(ETRI Secure E-commerce Service) 시스템[7,8]에서 각각 ESES/XKRS(XML-based Key Recovery System), ESES/Signature 및 ESES/Cipher 등의 서브시스템 형태로 개발되었다. 또한, ESES/Signature와 ESES/Cipher, 이 두 서브시스템에 제공되는 암호 라이브러리는 JCA(Java CryptoGraphy Architecture)[9,10]와 호환되는 ESES/jcrypto로 제공된다. 그리고, 키 복구 모듈인 ESES/XKRS 및 다른 서브시스템에게 제공하는 인퍼페이스는 ESES/XKRI (XML-based Key Recovery Interface)로 제공되고 있다.

[그림 6]은 ESES의 구조을 나타낸다.

ESES의 모든 서브 시스템들은 자바로 개발되었으며, XKRS 상의 모듈들을 제외하면 모두 API 형태이며 데이터는 XML을 사용한다. 따라서, ESES는 다양한 플랫폼에 이식 가능하고, 기존의 XML 기술 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하다. 그리고, 국제 표준 준수로 상호호환성을 제공하고, SEED, KCDSA 등의 국내 표준 암호 알고리즘들을 ESES/ jcrypto에 추가하여 국내외 어디에서나 적용 가능한 특징을 갖는다. XKRS의 모듈들에서 데이터 저장소, 키 저장소 및 키 복구 권한자 저장소 등은 MySQL로 구현되었으며, 사용자 모듈과 관리자 모듈은 Windows 환경으로 개발되었다. 키 복구 모듈인 KRM은 리눅스로



[그림 6] ESES의 구조

키 복구 서버로 구성하였다. 저장소 등은 간단한 인터페이스를 맞춰주기만 하면 다른 DB등으로도 확장이 가능하다.

VI. 결 론

본 논문에서 제시한 키 복구 모델은 B2B 시스템에서 적용하기 위해 설계된 것으로, 키 위탁 방식을 사용하며 기업에서 사용할 수 있도록 고안되고 개발되었다. 기업 간에 주고받는 서류를 W3C XML Encryption 그룹과 XML Signature 그룹에서 정의한 표준에 따라 XML 형태로 암호화하고 서명한다. 또한, 키 복구 시스템 내의 모든 인터페이스가 XML 형태로 이루어져 있다. XML 및 표준을 사용함으로써 보다 쉬운 인터페이스 및 시스템의 확장이 가능하며 다른 시스템과의 데이터 통합도 쉬운 장점을 가지며 기존의 XML 응용 및 XML 기반의 전자상거래 플랫폼에 투명하게 접목이 가능하다.

본 논문에서 구현된 키 복구 시스템은 내부 및 외부 키 복구 방법을 제공한다. 외부의 키 복구 방식은 자체 회사 내의 키 복구 모듈이 아닌 외부, 즉 거래가 있는 다른 회사들의 키 복구 모듈 등을 사용해서 그 거래에 해당하는 문서들을 복구하는 방법으로 자체 키 복구 시스템의 백업의 역할을 한다. 또한, 사용자가 키 복구 시스템을 사용하지 않고 다른 서명 및 암호 시스템을 사용하여 자체적으로 서명, 암호화하는 등의 악의적인 문서 조작에서 문서를 보호하는 역할을 한다.

마지막으로, 이 키 복구 방법을 구현한 ESES는 자바로 개발되었으며, XKRS 상의 모듈들을 제외하면 모두 API 형태이며 데이터는 XML을 사용한다. 따라서, ESES는 다양한 플랫폼에 이식 가능하고, 기존의 XML 기술 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하다. 그리고, 국제 표준 준수로 상호호환성을 제공하고, SEED, KCDSA 등의 국내 표준 암호 알고리즘들을 ESES/jcrypto에 추가하여 국내외의 다양한 알고리즘을 적용시킨 키 복구를 제공할 수 있다.

참 고 문 헌

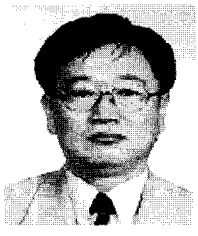
[1] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "*XML Signature Syntax and Processing*", http://

www.w3.org/TR/xmldsig-core/,2002
[2] Takeshi Imamura, Blair Dillaway and Ed Simon, "*XML Encryption Syntax and Processing*", http://www.w3.org/TR/xmlenc-core/, 2002
[3] Dorothy E. Denning, Dennis K. Branstad, "*A Taxonomy for Key Escrow Encryption System*", *ACM*, Vol. 39, No. 3, 1996.
[4] David Paul Maher, "Crypto Backup and Key Escrow", *Commuications of the ACM*, Vol. 39, pp. 48~53, 1996.
[5] Yoshiki Sameshima, "A Key Escrow System of the RSA Cryptosystem", *SCIS '98*, pp. 75~85, 1998
[6] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "*XML Key Management Specification (XKMS 2.0)*", http://www.w3.org/TR/xmldsigcore/, 2002.
[7] 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
[8] 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
[9] Sun, Java Cryptography Architecture API Specification and Reference, Oct, 1999.
[10] Sun, Java Cryptography Extension 1.2 API Specification and Reference, Mar, 1999.

〈著者紹介〉

김 주 한 (Ju-han Kim) 정회원
1997년 2월 : 충남대학교 컴퓨터과학과 졸업
1999년 2월 : 충남대학교 컴퓨터과학과 석사
2000년 8월~현재 : 한국전자통신연구원 능동보안기술연구팀
〈관심분야〉 전자상거래 보안, XML 보안, 워터마킹

문 기 영 (Ki-young Moon) 정회원
1986년 2월 : 경북대학교 전자공학과 졸업
1989년 2월 : 경북대학교 전자공학과 석사
1992년 1월~1994년 3월 : (주)대우정보시스템 기술연구소 대리
1994년 3월~현재 : 한국전자통신연구원 능동보안기술연구팀 선임연구원
〈관심분야〉 전자상거래 보안, 분산시스템, 트랜잭션



손 승 원 (Sung-won Sohn) 정회원
1984년 : 경북대학교 전자공학과 졸업
1994년 : 연세대학교 전자공학 석사
1999년 : 충북대학교 컴퓨터공학과 박사
1991년~현재 : 한국전자통신연구원 책임연구원(부장)
〈관심분야〉 네트워크 보안, 라우팅 알고리즘, 생체인식기술