제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

PKI기반의 전자결재시스템을 위한 계층적 그룹키에 관한 연구

성경상°, 오해석
숭실대학교 컴퓨터학과
actofgod@multi.ssu.ac.kr°, oh@comp.ssu.ac.kr

A Study on the Class Group Key for Electronic Approval System Based on PKI

Kyung-Sang Sung°, Hae-Seok Oh
Dept. of Computer Science, SoongSil University

요 약

정보화 물결이 일반화 되어가고 있는 이 시점에 있어 컴퓨터 통신망의 중요성은 두 말 할 나위가 없다. 일반 가정에서는 일상생활의 지혜와 정보교환이 우선시되어지고, 기업 내에서는 문서 양식의 통폐합 및 간소화 뿐만 아니라 기밀 사항이나 정보 교류가 일반화되어지고 있다. 하지만 문서의 결재방식에 있어서는 보안상의 문제점을 거론하며 번거로운 결재 방법을 이용하고 있다.
본 논문에서는 문서에 있어 전자결재의 순차적인 인증키 생성과 번거로운 인증 방식을 탈피하고자 그룹키를 생성하며, 그룹키를 이용한 단순하지만 보안상으로는 더욱 강력해진 방법을 제안하고자 한다.

1. 서 론

정보화는 우리들에게 PC를 통한 업무의 자동화나 인터넷을 통한 정보검색처럼 현실적인 변화로 다가오고 있으며, 이미 다른 선진국에서는 민원행정서비스나 그 밖의 여러 행정처리의 도입을 유도하고 있다. 이렇듯 정보화가 국가경쟁력을 높이기 위한 가장 중요하고 강력한 수단이라는 데는 이론의 여지(餘地)가 없다. 하지만 이러한 시스템의 도입은 되면, 첫째, 고객에 대한 신원확인의 문제점이 우려되고, 둘째, 전자문서의 무결성과 법적 효력에 대한 보장책임, 셋째, 거래 사실의 부인 방지를 해야 하며, 넷째, 시스템의 안전 및 신뢰성에 대한 사용자 신뢰를 확보하는 것이 선결문제인 듯 싶다. 이를 해결하기 위한 대안 중에 하나로 사용자 신뢰 확보를 위해 제시되고 있는 것이 PKI(공개키 기반 구조)구축과 이를 통한 전자서명 인증서비스의 도입으로 해결하고자 한다.

미국에서는 ACES(Access Certificates for Electronic Service)사업을 통해 개인 및 기업이 정부의 정보에 대한 접근 및 검색과 서류 제출 시 전자서명 기술을 이용한 신분확인과 인증과 부인방지 등을 제공하고 있다. 그 외 호주, 대만, 홍콩등지에서도 사무 자동화, 재택근무가 실현되고 있다. 이는 종이 문서를 사용하는 것 대신에 스크린을 통해 전자문서를 취급하는 전자 사무실이 도래한 것으로, 전자문서를 대상으로, 전자화 된 사무실에서 디지털 서명을 이용하여 결재를 수행하는 시스템을 전자결재 시스템이라 한다. 전자결재 시스템에서는 여러 사람들을 대상으로 하고 있으며, 이들이 생성해낸 전자 문서를 어떻게 주고받을지, 그리고 얼마나 안전하게 처리할지 등의 문제가 발생한다. 특히, 서로의 얼굴을 보지 않고서 모든 결재 행위를 수행하게 되므로, 제 3자에 의한 문서 위조, 네트워크 상에서의 정확한 문서 송신 여부, 그리고 수신자의 부정에 따르는 문제 등과 같이 여러 가지 보안 및 안전에 대한 선결 사항들이 필수적으로 처리되어야 한다.

현재 이에 대한 해결 방안으로 각광을 받고 있는 것 중에 하나가 PKI에 기반을 둔 디지털 서명이 있다. 이는 네트워크 상에서 전자 문서의 교환 시 발생할 수 있는 사용자 인증과 전자 문서 인증에 효과적인 해결책을 제시하고 있다. 그러나 기존의 디지털 서명 방식은 전자결재를 위해 서명자에서부터 최종결재자에 이르기까지의 키 생성과 키 확인 과정의 복잡성이 따르게 된다. 따라서 여러 사람을 대상으로 하는 다중 부서에서의 전자결재 시스템을 위해서는 기존의 디지털 서명으로는 부족하게 되었다.

이론적 배경을 통한 알고리즘은 2장에서 알아보고, 3장에서는 기존에 제시되었던 전자결재 시스템의 개요와 문제점들에 대해 서술하였다. 4장에서는 본 논문에서 제안하고자 하는 PKI기반의 효율적인 전자결재 시스템에 대해 알아보고, 이 시스템을 적용시켰을 경우 파생되는 이득에 대해 알아본다. 마지막으로 5장에서는 결론 및 향후 도입을 위한 시스템을 알아봄으로써

본 논문을 맺고자 한다.

2. 이론적 배경

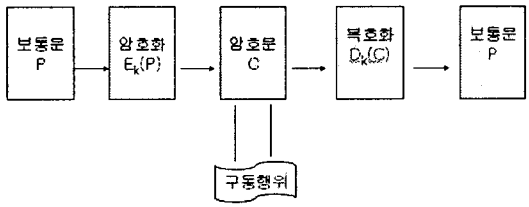
2.1 암호화 알고리즘

암·복호화 기법이란 비인가자가 알지 못하도록 평문을 암호문으로 변형시키고 허가자로 하여금 필요시에 다시 암호문을 평문으로 복호화 시킬 수 있도록 하는 체계를 뜻한다. 암호화 과정이란 평문이 암호문으로 되어가는 과정을 말하며, 암호문을 평문으로 만드는 과정을 복호화 과정이라 한다. 암·복호화가 이루어지는 구동 시스템을 살펴보면 다음과 같다.

■ 평 문 P ■ 암호문 C ■ 키 K

■ 암호화 알고리즘 E_k $E_k(P) = C$

■ 복호화 알고리즘 D_k $D_k(C) = P$



[그림 1 암·복호화 구동 과정]

암·복호화란 평문을 암호화알고리즘 과정을 거쳐 암호문으로 생성을 한 후, 상대방에게 보내게 되면 수신자는 수신되어진 암호문에 복호화 알고리즘을 적용시켜 원래의 평문으로 복화시키는 일련의 과정을 말한다.

암·복호화를 하는 방식에는 비대칭키 방식과 대칭키 방식이 있다. 대칭키 방식은 하나의 키만을 생성하여 서로간에 주고 받는 데이터에 대해 암·복호화하는 방식인데, 이 방식은 단 하나의 키만을 지니고 있어 일대일 방식에 사용되며, 키 값이 작으므로 암호화를 하는데 속도가 빠른 장점을 지니고 있는 반면에 기밀성이 떨어진다는 단점이 있다. 대칭키 종류에는 DES, 3-DES, AES, SEED 등이 있다. 비대칭키 방식은 키 생성 방식에 있어서 개인키와 공개키 두 개의 키를 생성을 한 후에, 개인키는 소유자가 지니게 되고, 공개키는 문서의 복호화를 위해 공시를 하게 된다. 이렇게 사용함으로써 얻어지는 장점은 단 두개의 키를 통해 일대다의 원활한 문서 교환을 이룰 수가 있으며, 키 값이 크므로 기밀성을 유지할 수 있는 반면에 암·복호화 시간이 지체된다는 단점을 지니고 있다. 비대칭키 종류에는 RAS, DH 등이 있다.

2.2 무결성을 위한 알고리즘

무결성이란, 데이터가 전달되는 도중에 데이터의 위·변조되지 않았음을 의미한다. 무결성을 위한 알고리즘에는 SHA-1 이나 MD5와 같은 해쉬 함수 종류가 있는데, 해쉬 함수의 처음의 취지는 데이터의 크기가 매우 크므로 상대방에게 전달하는데 네트워크의 부담을 줄이고자 도입되었으나, PKI 기반에서는 일방향 해쉬 기법을 도입하여 무결성을 입증하고자 하였다. 즉, 데이터 원본과 해쉬한 데이터를 같이 상대방에게 전달하면, 두 개의 데이터를 수신한 수신자는 원본의 데이터를 해쉬함수를 이용하여 해쉬한 값과 원래의 해쉬값을 비교하게 된다. 그래서 해쉬값이 다르다면 변질된 데이터임을 확인하게 되는 것이다. 이러한 방법을 통해 무결성을 검증하게 된다.

3. 기존의 전자결제 시스템의 개요와 문제점

3.1 PKI방식을 이용한 암호화 결재 방식

기안자는 서명을 하기 위한 일련의 과정인 랜덤 수 $R_1 \in Z_N$을 선택한다. 기안자는 X_i를 다음 서명자에게 전송한다. 서명자 n은 앞 서명자로부터 X_{n-1}을 수신하면 랜덤 수 $R_n \in Z_N$을 선택하여 계산하게 된다. 이렇듯 기안자로부터의 순차적인 키 생성 방식은 키 생성 시 기안자로부터 시작된 키 생성은 최고 결재권자에게까지 키 생성을 연결해야 하는 번거로움 뿐만 아니라, 키 생성 도중에 키 값이 변질된다면 전체적인 서명 절차를 이룰 수가 없게 되고, 키 생성을 처음부터 다시 시작해야 한다. 물론 기밀성에 있어서는 PKI기반을 중심으로 구축되어 있기 때문에 뛰어나지만 키 생성과 키 배포 단계에 있어 시간적인 지연 또한 발생하게 된다.

3.2 PKI방식을 이용한 키 생성 및 문서 암호화 과정

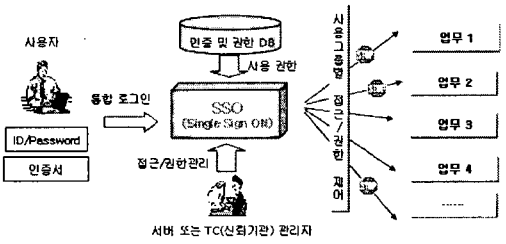
```
/* 키 생성 */
KeypairGenerator keyPairGenerator =
                        KeyPairGenerator.getInstance("RSA");
keyPairGenerator.init(1024);
KeyPair keypair = keyPairGenerator.genKeyPair();
-----------------
/* 생성된 키 파일로 저장 */
-----------------
/* 공개키 관리자에게 전송하여 게시 */
-----------------
/* 공개키로 문서 암호화 */
X509EncodedKeySpec keySpec =
                        new 509EncodedKeySpec(keyBytes);
KeyFactory keyFactory = KeyFactory.getInstance("RSA");
PublicKey publickey = keyFactory.generatePublic(keySpec);
```

[일반적인 키 생성 및 암호화 방법]

4. PKI 기반의 효율적인 전자결재 시스템

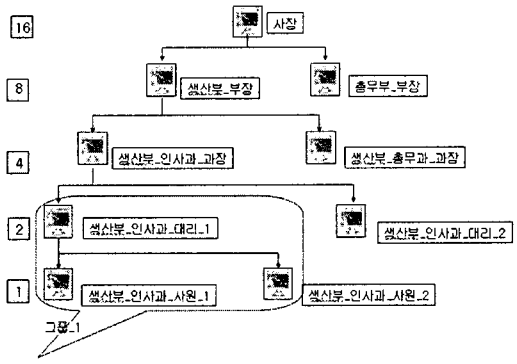
4.1 시스템 개요

제안하는 시스템에서는 문서에 대한 등급의 개념을 이용하는데, 보다 융통성 있는 결재력을 지닐 수 있도록 하기 위함이다. 기밀문서, 일반문서, 긴급문서 그리고 우선적이면서도 기밀을 요하는 문서로 나눌 수 있는데, 기밀문서는 보다 중요한 문서이므로 암호화 수준을 높인 이중 암호화 방식을 채택을 한다. 이중암호화라 함은 데이터를 상대방의 공개키로 암호화를 하고, 그 암호문을 보내고자 하는 상대방의 그룹 공개키를 덧붙임으로써 데이터의 기밀성을 한층 더 높이기 위한 수단에 초점을 맞춘 것이다. 또한 기밀성을 한층 더 높이기 위한 수단으로 인증키 생성 과정을 사용자를 기준으로 설정하였다. 기존에는 서버 또는 신뢰기관(TC : Trust Center)이 담당해서 키를 생성한 후에 공개키는 자신이 보관하고 담당자에게 개인키를 배분하는 형식으로 되어 있는데, 반면에 제안된 시스템에서는 담당자가 직접 인증키를 생성한 후 서버 또는 TC에게 공개키를 주는 형식으로 설계되어 있기 때문에 사용자를 위한 기반에 우선권을 부여했다. 또한 그룹키에 관한 키생성은 TC에게 일임하는 형식을 취해서 TC와 사용자간의 공생을 유지하고자 했다. 일반문서는 비대칭키 암호화방식을 채택해서 전송하게 되고, 긴급문서에는 우선권을 부여한다. 기밀문서이면서 우선권을 요하는 문서에는 이중암호화 과정과 우선권을 부여해서 전송하게 된다. 그림 2는 로그인해서 접속한 후에 갖게되는 권한 부여에 관련된 일련의 과정을 보여준다.



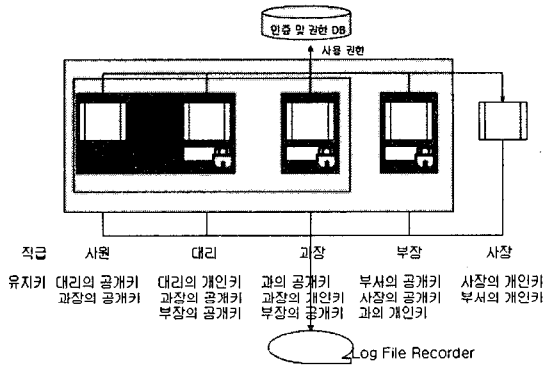
[그림 2 접속 과정]

그림 3은 결재시스템의 계층적 구조도를 도식한 것으로서 옆에 있는 숫자는 결재에 관련된 모니터링을 통해 확인하는 수준에서 문서에 서명된 수치만으로도 확인할 수 있도록 하였다.



[그림 3 결제 시스템 계층도]

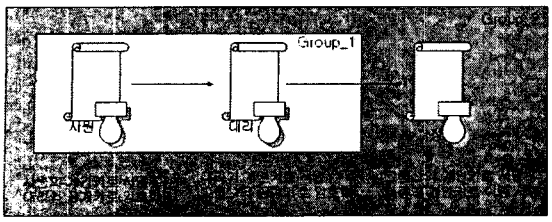
예를 들면, 사원을 거쳐 과장의 서명과 부장이 서명을 했다면, 13이라는 수치가 문서에 붙게 된다. 그것만으로도 DB 확인 없이 서명 과정을 확인하게 되는 것이다. 이렇게 함으로써 보다 신속한 서명 절차를 거치는 과정을 모니터링 할 수 있게 된다. 그림 4는 PKI를 기반으로 결재 시스템을 도식화 한 것으로써 각 책임자들의 개인키와 공개키 뿐만 아니라 그룹에 할당되어진 고유의 그룹 키를 지니고 있는 것을 보여주는 것이다.



[그림 4 PKI 기반의 결재 시스템 구조도]

그룹키 생성 과정은 부서에 할당되어진 고유 ID number와 TC관리자가 RNG를 통해 얻어낸 임의로 생성시킨 일련의 number를 XOR 시킨 후에 생성된 값으로 키 값을 생성시키게 된다. 그런 후 생성된 그룹키는 부서책임자들에게 보내지게 된다.

그림 5에서는 생성되어진 인증키를 통한 문서의 결재 순서 부분을 상세하게 도식화했다.



[그림 5 결재 순서]

사원은 자신의 개인키로 서명을 하고 상급자인 대리의 공개키로 암호화를 한다. 그런 다음 원본의 해쉬값과 함께 대리의 공개키로 암호화를 한 후에 대리에게 보내지게 되면 상급자인 대리는 자신의 개인키로 복호화를 한 후에 다시 사원의 공개키로 서명을 풀게 된다. 그런 다음 해쉬되어진 값을 비교함으로써 무결성을 입증하게 되는 절차를 거친다. 입증되어진 데이터는 그룹 1의 개인키로 서명을 하고, 그룹 2에 속해 있는 상위의 결재권자의 공개키로 암호화한 후에 송신하게 된다. 만약 기밀서류인 경우에는 그룹 2의 공개키로 다시 한번 암호화를 하는 수준까지 가게 된다.

5. 결론 및 향후 과제

최근 인트라넷은 기업의 효율적인 사무 환경 구축의 대안으로 떠오르고 있다. 이를 이용한 전자결재시스템은 인간과 업무간에 조화롭게 일을 수행하는 환경을 만드는 것으로 시스템이 사람과 작업단위 사이에서 중재자 역할을 수행 담당하게 된다. 시스템이란 매개체를 통한 작업이기 때문에 신뢰라는 단어를 무색하게 만들기도 한다. 그럼으로 보안이란 개념의 중요성이 떠오르게 되고, 본 논문에서는 보안이란 개념에 맞추어 암호화 수준을 높이고, 사용자를 우선시하는 입장에서 시스템을 구축하고자 하였다. 이런 인프라를 구축함으로써 보다 향상된 사용자 기반의 결재시스템을 구축하게 되며, 이 시스템은 보안을 중요시 여기는 국가 정부 기관에도 충분히 활용할 수 있을 것으로 여겨진다.

참고 문헌

[1] 박희운, 강창구, 이임영 "디지털 다중서명 방식을 적용한 전자결재 시스템에 관한 연구", 한국정보처리학회 논문지, 제6권, 제4호, pp.999.-1008, 1994.

[2] 장용철, 오태석, 오무송, "암호화를 이용한 전자결재 시스템의 설계 및 구현", 한국정보처리학회 논문지, 제4권, 제6호, pp.2060-2069, 1997

[3] 박 용 "주요국전자민원행정서비스의 전자서명인증 도입 현환" 한국정보보호진흥원 정보보호 기술 및 정책동향, 2001

[4] Gartner Group Inc., "Accelerating Internet Securities Trading Adoption in Asia/Pacific", Research Brief, Apr. 10, 2000.

[5] IDC, Security Products in Use and Planned for Use", IDCs 1998 Internet Security Survey, 1999

[6] Dream Security, "http://www.dreamsecurity.com/"

[7] Secure Soft, "http://www.securesoft.co.kr"

[8] 보안 기법에 대한 기술 정리 "http://my.netian.com/%7Eaphise/security/security.html"

[9] Doris Baker, H.X.Mel, 정재원 역, "보안과 암호의 모든 것", 인포북, 2001