제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

전자인증기반 교육행정정보시스템 설계

노선진, 정일용
조선대학교 전자계산학과
ksknsj1@hanmail.net, iyc@mina.chosun.ac.kr

A Design of Digital Authentication-based NEIS

Seon-Jin No Il-Yong Chung
Dept. of computer science, Chosun University,

요 약

교육행정업무에 대한 전자적인 거래 혹은 각종 문서의 안전한 송·수신과 사용자의 신원을 확인하여 안전한 행정업무 수행이 가능하도록 하기 위해서는 보안을 갖춘 인증체제를 도입하였다. 본 논문에서는 PKI 기반 암호기술를 이용하여 전자인증기반의 교육행정정보 시스템을 설계하였다. 세부거래에 대한 알고리즘은 비밀키, 키 교환 공개키, 개인 키 및 서명용 공개키· 개인 키를 사용하였고 또 시스템 지원 기관의 서버가 사용자의 신원을 확인할 수 있어서 업무담당자 및 관련자의 안전한 업무수행 보증과 국민에게 교육행정정보 및 민원서비스를 안전하게 제공하는 교육행정정보 시스템을 설계하였다. 제안된 시스템의 인증모듈은 인증, 기밀성, 무결성, 부인봉쇄 서비스 등의 보안기능을 제공하도록 설계되었다.

1. 서 론

교육행정의 정보화 및 대국민 서비스의 강화로 각종 민원 사항에 대한 시간과 지역에 관계없는 One / Non-Stop 처리를 가능하게 하여 국민의 편익 증진, 각 16개 시/도교육청 단위시스템의 통합을 지향하고 교육행정 업무 절차를 간소화함으로써 교육행정의 생산성 및 투명성 제고, 교육행정정보시스템 전반의 인프라 및 업무개선을 통한 전자정부기반 강화를 목적으로한다. 웹기반의 환경으로 구축되는 교육행정정보시스템은 관련기관 및 관련부처, 학부모, 학생, 기타 민원인 등을 대상으로 다양하고 광범위한 경로를 통해 서비스를 제공하므로 많은 보안상의 위협에 노출될 수 있다[4].

따라서 침입차단 시스템과 침입탐지 시스템을 도입하여 네트워크 보안을 강화하며 PKI 기반의 접속인증, 전자서명, 암호화[5,6,7]를 적용하고 서버보안 시스템을 도입해 서버보안을 강화하는 등 최적의 보안관리 시스템을 구축함으로써 교육행정정보시스템의 신뢰성을 확보한다[4].

이에 따라 정부 전자관인 기반(GPKI)과 인증기관 기반(NPKI)의 인증 인프라를 사용하고 공인인증기관의 시점확인서버 시간을 사용함으로써 분산된 사용자의 설정된 시간이 다름으로 인해 데이터를 주고받는 상호간에 혼란과 데이터 생성시간에 대한 논란을 최소화하여 시스템에 대한 신뢰성을 증가시킨다. 또한 ON-LINE상의 인증서가 필요한 실제 사용자에 대한 공인인증기관의 신원확인 서비스[6]를 이용하여 비인가자에 의한 인증서 불법도용 및 개인정보 유출을 방지하여 시스템의 신뢰성을 증가시킨다[4].

2 전자서명 인증기술

2.1 전자서명의 개념

컴퓨터 네트워크를 통한 비대면 방식의 전자적거래는 대면방식의 기존 거래 방식의 단점을 극복할 수 있게 한다. 전자적 거래는 기존 거래 방식에서 시간적·공간적 제약의 문제점을 해결해 줌으로써 새로운 거래 문화로서 자리잡아 가고 있다. 그러나, 전자적 거래는 많은 순기능이 있음에도 불구하고, 사용자에게 역기능을 제공할 수 있다는 문제점 때문에 보안 요구사항이 선결되어야만 전자적 거래의 활성화를 기대할 수 있을 것이다. 정보보호 역기능을 방지하기 위하여 필요한 대표적인 정보보호 서비스

는 [표1]과 같다.

전자서명은 상기의 보안 요구사항중 인증, 무결성, 비밀성, 부인방지에 대한 보안 기능을 제공해 주며, 이것은 결국 비대면 방식의 전자적 거래 환경 구축 시 전자서명 기술이 필요하다는 것을 의미하는 것이다[1].

[표 1] 정보보호 서비스 분류

구 분	내 용	필요기술
인증 (*Authentication*)	사용자 인증 : 정당한 사용자 메시지 인증 : 메시지 진정성	전자서명
무결성 (Integrity)	메시지 진정성	전자서명
비밀성 (Confidentiality)	정당한 사용자만이 메시지 확인 가능	암호화
부인방지 (Non-repudiation)	메시지 작성 또는 송·수신에 대한 부인 불가능	전자서명

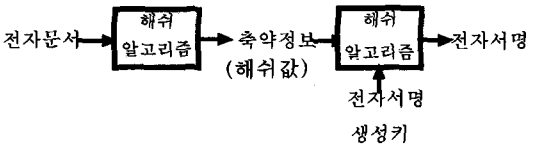
2.2 전자서명 인증의 필요성

인증(Certification) 서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 안전한 전자상거래 환경의 구축을 위해서는 앞에서도 언급한 바와 같이 인증, 무결성, 비밀성, 부인방지 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다. 현재 안전성을 정량화 시킬 수 있는 공개키 암호방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증 서비스가 필요하게 된다.

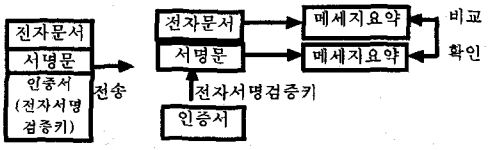
인증기관은 전자서명을 이용하고자 하는 사용자들에 대하여 전자서명검증키(공개키)가 해당 사용자의 소유임을 증명하고 또한 해당 키가 위·변조 되지 않았다는 사실을 증명하기 위하여 전자서명검증키와 사용자 정보 등으로 구성된 데이터에 전자서명을 수행함으로써 인증서를 생성한다[1].

2.3 전자서명 생성 및 검증

전자서명을 하기 위해서는 먼저 전자서명에 사용할 한 쌍의 전자서명 생성키 및 검증키를 생성해야 한다. 전자서명 생성키는 개인별로 보관·관리하고, 전자서명 검증키는 전자문서 수신자에게 공개(검증키가 포함된 인증서를 공개)한다. 통상적으로 서명키는 비밀유지 및 이용편의를 위해 IC카드에 저장하며, 데이터 축약 알고리즘(일방향 해쉬알고리즘)을 사용하여 전자문서를 요약한 일정한 길이의 축약정보(해쉬값)를 생성하게 되는데, 많은 양의 문서 전체를 서명하게 되면 상당한 시간이 소요되므로 전자서명을 효율적으로 수행하기 위해 문서를 축약하여 전자서명한다. 통상 축약정보의 길이는 128~160비트이며, 전자서명 생성 알고리즘과 서명자의 서명생성키를 사용하여 전자문서의 축약정보에 전자서명을 하고 서명문을 생성한다.



전자서명에 대한 검증은 검증 알고리즘과 서명자의 서명검증키를 사용하여 수신된 전자서명으로부터 전자문서 축약정보(해쉬값)의 복원을 통해 가능하다. 수신자는 송신자의 전자문서와 함께 전송된 인증서(인증기관 발급)에 포함된 전자서명검증키를 이용하여 축약정보를 복원할 수 있다. 수신자가 생성한 전자문서의 축약정보(해쉬값)을 서명자가 서명하여 전송한 축약정보와 비교함으로써 서명자의 신원 및 전자문서 위·변조 여부를 확인하게 된다[2].



3. 전자인증기반 교육행정정보시스템 설계

3.1 PKI을 이용한 인증서 발급 및 확인 프로토콜

교육행정정보시스템에서 PKI 암호화기술을 이용한 전자인증기반 교육행정정보시스템을 제안한다. 제안하는 프로토콜의 표기법은 [표2]과 같다[3,5,6,7].

교육행정정보시스템 서버는 인증기관에서 서버 인증서을 발급 받는 단계는 기술하지 않았다. 그리고 인증 서비스하는 기관에서 제공하는 보안 모듈 프로그램은 다양한 환경의 응용 프로그램 개발시 인증과 보안기능을 구현하고자 하는 경우에 해당되는 보안기능을 수행 할 수 있으므로, 보안과 관련된 전문지식이 없더라도 쉽게 사용할 수 있다. 사용자는 이 보안 모듈 프로그램만 설치하여 요청하면 된다.

[표 2] 제안된 프로토콜 표기법

표기	설명
U	교육행정정보시스템 사용자(user)
CA	인증기관(Certificate Authority)
RA	등록기관(Registration Authority)
BRA	등록지원기관(Registration Authority)
DS	인증서 저장소(Directoy Server)
S	교육행정정보시스템 서버
ID	사용자 등록명(Indentification data)
RESULT	인증승인 결과
UI	사용자 정보(이름,주민등록번호,전화번호)
EDB	교육행정정보시스템 사용자 DB
DS	인증기관 Directory Server
ULA	사용자 로그인 승인
$Auth_i$	i에 대한 인증서
RN	인증기관에서 발급한 참조번호 (Reference Number)
SC	인증기관에서 발급한 인가코드(Sanction Code)
ID_i	i의 식별자
PK_i	i의 공개키
SK_i	i의 개인키
$Auth_i$	i의 인증서
$E_k[M]$	k를 이용하여 M을 암호화
$D_k[M]$	k를 이용하여 M을 복호화
h(M)	M을 해쉬함수로 수행
$Time_i$	타임스탬프
M_1	사용자 ID || 사용자 PASSWD

[각 단계별 Transaction 표기]

○ 인증서 발급 단계

[단계 1] U → BRA : UI

[단계 2] BRA → RA : UI

[단계 3] RA → EDB : UI

[단계 4] RA → CA : UI

[단계 5] CA → RA : RN, SC

[단계 6] RA → BRA : RN, SC

[단계 7] BRA → U : RN, SC

[단계 8] U → CA : $PK_{CA}[RN, SC, PK_u]$

[단계 9] CA → U : $Auth_u$

where $Auth_U = E_{SK_{CA}}[Time_i, ID_U, PK_U]$

[단계 10] U : $Auth_u$

[단계1] 사용자는 등록지원기관에 신원확인 및 사용자 등록 요청을 한다.

[단계2] 등록지원기관은 사용자 신원확인 후 등록기관에 사용자 등록요청을 한다.

[단계3] 등록기관은 사용자의 신원확인 후 DB서버에 사용자 정보를 저장한다.

[단계4] 등록기관은 인증기관에 인증서 발급을 위하여 인증기관 서버로 전송하여 등록한다.

[단계5] 인증기관은 등록 처리 결과인 참조번호 및 인가코드를 등록기관으로 전송한다.

[단계6] 등록기관은 등록 처리 결과인 참조번호 및 인가코드를 등록지원기관으로 전송한다.

[단계7] 등록지원기관은 참조번호 및 인가코드를 사용자에게 off-line으로 통보한다.

[단계8] 사용자가 CA에 인증서 발급요청을 하면 자동으로 인증기관 보안 프로그램이 설치되면서 인증기관의 서명용 공개키가 사용자 컴퓨터에 다운 되면 사용자는 서명용 키쌍 생성 후 5. 항에서 받았던 내용과 서명용 키쌍 중 공개키를 인증기관 공개키로 암호화하여 인증서 발급 요청을 인증기관에 한다.

[단계9] 인증기관에서는 인증기관 서명용 개인키로 복호화하여 요청자 확인, 공캐키 유일성 검증의 인증서 요청 메시지를 검증하여 사용자의 정보, 사용자 서명용 공개키, Time-stamp등을 포함한 인증기관 서명용 개인키로 구성된 인증서를 생성· 발급하고 디렉토리 서버에 인증서 게시를 등록한다.

[단계10] 사용자는 보안 모듈 프로그램을 이용하여 수신 후 사용자 인증서 저장장소에 저장한다.

○ 인증서 승인 및 사용 단계

[단계 1] U → S : $E_{SK_U}[h(M_1)], Auth_U$

[단계 2] S : $D_{PK_{CA}}[Auth_u]$

$D_{PK_U}[h(M_1)]$

[단계 3] S → CA : $E_{SK_S}[Auth_U]$

[단계 4] CA → S : RESULT

[단계 5] S → U : ULA

[단계 6] U → S : $E_{SK_U}[h(M_2)], Auth_U$

where M_2 = request message of work

[단계 7] S → U : $E_{SK_S}[h(M_3)], Auth_S$

where M_3 = result message of work

[단계1] 사용자가 ID, Passwd를 사용자 개인키로 암호화한 전자서명, Timestamp가 포함된 인증서 로그인 정보를 서버로 전송한다.

[단계2] 서버에서는 사용자의 인증서를 인증기관의 서명용 공개키로 복호화 후 사용자의 서명용 공

개키로 ID, Passwd를 복호화 하여 전자서명 검사, 인증서의 유효성 및 신원확인을 검사하고 검사결과를 응용 프로그램으로 전달 응용프로그램은 사용자 등록 DB에 사용자등록 여부를 확인한다.

[단계3] 서버는 사용자의 인증서 내용을 인증기관 DS서버로 전송한다.

[단계4] 인증기관의 DS서버에서 인증서 유효기간 확인, 폐기여부 등의 유효성을 검증하여 그 결과를 서버에 전송한다.

[단계5] 서버는 사용자가 맞으면 로그인 승인처리를 한다.

[단계6] 사용자가 해당 작업 처리 내용을 서명용 개인키로 암호화하여 사용자 인증서와 같이 전송한다.

[단계7] 서버는 서명용 개인키로 저장결과를 암호화하여 서버 인증서와 함께 전송한다[7].

3. 2 프로토콜 분석

제안한 프로토콜을 통한 교육행정정보시스템은 기밀성, 인증, 무결성, 부인봉쇄 서비스 등을 제공할 수 있다.

기밀성은 *[단계6]*과 같이 자료들을 서로 암호화 및 전자서명으로 보내 전송되는 모든 데이터를 안전하게 다른 사용자의 도청으로부터 보호한다.

인증은 1차적으로 인증서 삭제등을 대비하여 USB-key, 스마트카드 등에 암호화하여 저장한다. 2차적으로 교육행정정보시스템 서버에 접속하는 시점에 [단계1]부터 [단계4]와 같이 인증서 확인 절차를 거쳐 교육행정정보시스템 서버로 전송하게 된다. 그리고 사용자와 교육행정정보시스템 서버간의 인증은 신뢰된 인증기관으로부터 발부 받은 인증서를 전송하여 인증기관 전자서명 검증키로 복호화하여 검증한다.

무결성은 거래 정보가 변경 되었을 때 확인 할 수 있는 방법이다. [단계6], [단계7]와 같이 Data을 사용자의 개인키로 전자서명 암호화하여 인증서와 함께 보내면 인증서를 인증기관의 공개키로 복호화 후 인증서에 포함되어 있는 사용자의 공개키로 data를 복호화 하는 서명검사를 통해 DB에 Data만 저장한다.

부인봉쇄는 [단계6], [단계7]와 같이 거래 정보를 개인키로 서명함으로써 이루어지는데 수신부인봉쇄는 수신확인 Data 내역과 수신자 전자서명를 이용하여 인증서를 사용하여 전자서명을 검사함으로써 확인하고 발신부인봉쇄는 데이터내역과 발신자 전자서명을 이용하여 인증서를 사용하여 전자서명을 검사함으로써 확인한다.

4. 결론

사용자 측면에서의 보안 요구사항을 분석하고, 이에 적합한 교육행정정보 시스템의 사용자 보안 기능을 설계하였다. 그리고 인터넷을 기반으로 한 교육행정정보시스템 서비스에서 고유문제를 제시하고 그에 필요한 인증기술 및 보안기술을 제시하였다. 인터넷을 통한 교육행정정보시스템 실현을 위한 선결 기술요소 중 보안 기술에 대한 분야의 기술 확보가 시급히 요청되는 시점이며, 특히 인증에 대한 기반 기술의 확보는 교육행정정보시스템의 서비스에서 요구되는 사용자의 신원 확인과 사용 내역의 증명 등에 활용되는 기반 기술 요소이다.

세부거래에 대한 알고리즘은 비밀키, 키 교환 공개키, 개인 키 및 서명용 공개키· 개인 키를 사용하였고 또 시스템 지원 기관의 서버가 사용자의 신원을 확인할 수 있어서 업무담당자 및 관련자의 안전한 업무 수행 보증과 국민에게 교육행정정보 및 민원서비스를 안전하게 제공하는 교육행정정보 시스템을 설계하였다. 그리고 이 논문에서는 기술하지 않았지만 권한관리자를 두어 각 사용자 별로 권한을 부여하여 업무별 보안을 확보하였다.

본 논문은 교육행정정보시스템에 인증 프로토콜을 제안하였으나 앞으로 상호 인증에 필요한 프로토콜 및 소프트웨어를 개발하여 인증, 비밀성, 부인송쇄, 무결성 등은 향후 중점적으로 연구가 필요하다.

5. 참고문헌

[1] 최영철 외 2인, "전자서명법과 전자서명 인증관리체계" ,한국정보과학회, 제18권 제1호, pp.0013~0020, 2000. 1.

[2] 나희동, "한국증권전산 공인인증기관", 한국정보과학회, 제18권 제5호, pp.0068~0070, 2000. 5

[3] 김석우 외1인, "전자상거래 인증서비스 기술", 한국정보처리학회, 제7권 제2호, pp.0020~0024, 2000.3

[4] 삼성 SDS, "교육행정정보시스템 기술제안서", 2002.

[5] http://www.kisa.or.kr

[6] http://sign.nca.or.kr

[7] http://www.signgate.com