Journal of the Korean Institute of Industrial Engineers
Vol. 26, No. 4, pp. 411-420, December 2000.

PKI를 이용한 CITIS 사용자 인증 시스템

정우필 · 박정선

명지대학교 산업공학과

A Certification System Using PKI for CITIS Users

Woo-Phil Jung · Jung-Sun Park

Among the standards of CALS, CITIS(Contractor Integrated Technical Information Service) is a standard in information share procedure which manages all data and services occurred between a contractor and a purchaser. CITIS services have some security problems like authentication problem and repudiation problem, when they are implemented using the Internet. To solve these problems, CITIS needs a user certificate system which can allow to access important information only to qualified users.

This paper proposed a PKI(Public Key Infrastructure) Certificate Authority for CITIS, and created a real User Certificate System which can be adjusted to circumstances of real CITIS.

1. 서 론

정보기술의 급속한 발전과 더불어 근래에는 정보기술을 이용한 전자적 상거래에 대한 많은 연구, 개발과 상용화가 이루어지고 있는 실정이다. 그 중에서도 CALS의 서비스 표준인 CITIS의 구현이 각 산업부분별로 활발하게 이루어지고 있다.

CITIS(Contractor Integrated Technical Information Service)는 CALS의 여러 표준 중에서 서비스 표준, 즉 CALS 데이터의 Service Gateway라고 할 수 있다. CITIS는 CALS를 구현하는 과정에서 제품 및 시스템을 발주하는 발주자와 발주자의 요구에 따라 제품 및 시스템을 납품하는 공급자 사이에서 계약에 따라 발생하는 기술 정보 및 비즈니스 정보를 공급자는 전자적으로 제공하며, 발주자는 전자적으로 접근 가능한 기능을 제공하여 상호 규정된 정보를 자동적으로 교환하는 것이다. 즉 CITIS는 공급자가 발주자의 데이터베이스에 접근 가능하도록 발주자가 제공하는 서비스로, 공급자가 필요한 전자화된 데이터의 사용이 가능하고 컴퓨터 소프트웨어 및 하드웨어의 제공 등을 포함하는 모든 활동과 기능을 갖는다.

이렇게 전자 상거래에서 발생하는 데이터의 전자적인 교환을 담당하는 CITIS에서도 근래에 대두되고 있는 정보의 보호가 절실히 요구되고 있다. 특히 CITIS가 인터넷을 기반으로 조성되어 있고 이러한 정보환경에서는 정보의 개방성을 기본으로 하기 때문에 정보망에서 유통되는 메시지에 대한 가로채기, 도청, 위조, 신원 사칭 등과 같은 불법적인 행위에 대한 위험성이 상존하고 있어 이에 대한 해결책이 절실히 필요한 상태이다.

본 논문에서는 이러한 개방적인 환경에서 CITIS 보안의 문제를 해결하기 위한 방법으로 인증된 사용자들만이 CITIS에 접근하도록 하는 CITIS 사용자 인증 시스템 구현 방안을 제시하고, 실제로 구현된 CITIS Prototype에 사용자 인증을 하여 주는 절차를 추가하여 CITIS 사용자 인증 시스템을 구현하였다.

사용자 인증 기술은 이제 Internet에서 정보보호 기술로써 널리 사용되고 있다. 예전까지 사용자 인증은 주로 ID와 패스워드를 사용한 것이었으나 이것은 정보 기술이 발전함에 따라서 보안상에 많은 문제점을 보이게 되었다. 현재 사용하고 있는 암호 시스템은 대칭키 암호 시스템과 공개키 암호 시스템이다. 대칭키 암호 시스템을 이용하는 사용자 인증 체계는 다수의 사용자에 대해 각 사용자마다 키를 관리해야 하는 어려움이 있다. 그러한 키 관리 어려움을 해결하기 위하여 인증기관(Certificate Authority : CA)을 이용한 사용자 인증체계는 공개키 암호화 알고리듬을 사용한 공개키 기반구조(Public Key infrastructure : PKI) 인증기관을 사용한다.

공개키 기반구조를 이용한 사용자 인증 시스템은 주로 단일 소프트웨어로서 개발되고 있는 실정이다. 해외 인증 소프트웨어 제품 개발은 주로 미국과 캐나다가 주도하여 이미 많은 제품이 출시되어 있는 상태이고, 최근 들어 유럽연합에서 국가간 공동 연구가 활발히 진행됨에 따라 유럽제품들도 많이 개발되어 판매되고 있다. 대표적인 제품으로는 미국의 Netscape Certificate Server, BBN CAW, CyberTrust사의 GTE Global Provider CA, 캐나다의 Sentry CA와 Entrust/WebCA, 스웨덴의 Notary

Certificate Authority, 독일의 SECUDE CA Management 등이 있다.

한편, 인증 소프트웨어에 대한 국내 제품 개발은 1997년부터 시작하여 최근에 다수의 제품들이 출시되고 있으며 몇몇 제품의 경우에는 실제 국내 전자 상거래 서비스에 적용되어 있기도 하다. 국내의 대표적인 인증 소프트웨어는 이니텍의 CA 서버, 장미디어 인터렉티브의 JMI CA, 삼성 SDS의 TrustPro 등이 있다.

국내 인증 소프트웨어들도 해외 인증 소프트웨어들과 유사한 기능과 표준 기술을 적용하고 있으면서도 한국 표준 전자서명 알고리듬(KCDSA)을 추가적으로 지원하고 있는 것이 특징이다.

CITIS 개발에 대한 사례로는 국내의 경우Electropia의 CITIS 프로토타입과 건설 CALS의 CITIS 프로토타입이 있으며, 외국에서는 CITIS로 사업을 하고 있다(McDonell Douglas의 자회사인 AeroTech).

그러나 모두 PKI를 이용한 CITIS는 없다. CITIS는 계약자가 조달자에게 제공하는 고가이면서 비밀인 정보를 제공하는 경우가 있다. 예를 들어, 첨단산업에서 제조를 하청받은 경우가 그렇다. 이럴 경우 인증은 일반 상거래에서의 인증보다 훨씬 강화된 인증 시스템이 요구된다.

2. 인증 기반 기술

2.1 암호 시스템

암호 시스템은 암호화되지 않은 상태의 원문을 암호문으로 만드는 암호화와 반대로 암호문을 원문으로 변화시키는 복호화, 그리고 이 과정 속에 사용되는 암호화 키와 키의 관리 등 전자적 데이터의 보호를 위한 일련의 프로세스들을 일컫는 말이다. 이러한 암호 시스템은 전자적 데이터와 데이터 전송에 관한 정보의 비밀성을 제공할 수 있고, 다른 보안 응용 활용에서 중요한 역할을 담당하기 때문에 암호 시스템은 다음 세 가지 요건을 충족시켜야 한다.

- 키에 의하여 암호화 및 복호화가 효과적으로 수행되어야 한다.
- 이용하기에 용이하여야 한다.
- 암호 시스템의 알고리듬 자체보다는 암호 키에 의한 보안이 이루어져야 한다.

암호 시스템에 사용되는 암호화 알고리듬에는 두 가지가 있다.

- 암호화와 복호화 키가 같은 대칭키 암호 시스템
- 암호화 키를 안다고 해도 복호화 키를 알 수 없는 공개키 암호 시스템(Ahuja, 1997; Cericom; IETF Draft, 1998)

2.2 전자서명

전자서명(Digital Signature)이란 종래의 인감도장, 혹은 사인처럼 개인의 고유성을 주장하고 인증 받기 위해 전자적 문서에 서명하는 방법을 말한다. 전자 서명에 대한 조건 및 특징은 <표 1>과 같다(Ahuja, 1997; Cericom; IETF Draft, 1998).

표 1. 전자서명의 조건 및 특징

조 건	특 징
· 서명은 서명되고 있는 메시지에 의존하는 형태이어야 한다. · 위조와 부인을 방지하기 위해 송신자에게 있어서 유일한 어떤 정보를 이용해야만 한다. · 서명을 만들기가 비교적 쉬어야 한다. · 서명을 인식하고 확인하기가 쉬어야 한다. · 전자 서명을 위조하는 것이 계산적으로 실행 불가능해야 한다. · 기억 장소에 전자 서명의 복사본을 유지하는 것이 실용적이어야 한다.	· 그 서명의 저자와 날짜와 시간을 확인 할 수 있다. · 서명할 때의 내용을 인증할 수 있다. · 서명은 분쟁을 해결하기 위해서, 제삼자에 의해서 확인될 수 있다.

2.3 해쉬 함수

해쉬 함수는 임의의 긴 문자열을 고정된 길이의 값으로 바꾸는 함수이다.

- 해쉬 출력값을 이용해 원래의 입력값을 추정하는 것은 계산상으로 불가능해야 한다.
- 입력값과 해당 해쉬 출력값이 있을 때 이 해쉬 출력값에 해당하는 또 다른 입력값을 구하는 것은 계산상으로 불가능해야 한다.
- 같은 해쉬 출력값을 갖는 두 개의 다른 입력값을 발견하는 것은 계산상 불가능해야 한다.

2.4 공개키 기반구조

전자서명 기술은 공개키 암호 시스템으로 비밀키와 공개키가 사용된다. 공개키는 공개된 정보이므로 어떻게 공개키의 위/변조 문제를 해결하는가 하는 공개키 인증 문제로 귀착된다. 이러한 공개키 인증문제를 해결하기 위해 나온 것이 공개키 기반구조이다(DoD, 1993; NIST,1994).

2.4.1 공개키 기반구조의 정의

공개키 기반구조는 정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용분야에서 인증서(Certificate)의 사용을 용이하도록 하는 정책, 수단, 도구 등을 수립하고 제공하는 객체들의 네트워크이다.

공개키 기반구조는 다음의 5가지 기본 보안 서비스를 제공한다.

표 2. 공개키 기반구조의 구조와 역할

구 조	역 할
인증기관	인증기관은 공개키 기반구조를 구성하는 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 정책승인기관(PAA: Policy Approving Authority), 정책인증기관(PCA: Policy Certification Authority), 인증기관(CA: Certification Authority) 등 세 가지 기관을 모두 통틀어 인증기관이라고 한다.
등록기관	인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 등록기관을 두어 인증기관 대신 사용자들의 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행한다.
디렉토리	인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서취소목록 등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다.
사용자	PKI 내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다

- 프라이버시 : 정보의 기밀성을 유지한다.
- 접근제어 : 선택된 수신자만이 정보에 접근하도록 허락한다.
- 무결성 : 정보가 전송 중에 변경되지 않았음을 보장한다.
- 인증 : 정보의 원천지를 보장한다.
- 부인봉쇄 : 정보가 송신자에게 전송되었음을 보장한다.

2.4.2 공개키 기반구조의 구성

공개키 기반구조를 구성하는 최소 객체들은 인증기관, 등록기관(RA:Registration Authority), 디렉토리, 사용자이다.

위의 <표 2>는 공개키 기반구조의 구성과 그 역할에 대한 설명이다.

2.5 인증기관

2.5.1 CA의 구조

인증 구조란 CA들 사이의 관계를 나타낸 것이다. 여러 가지 기술적, 경제적 이유로 인하여 세계에서 하나의 CA만이 존재한다는 것은 불가능하기 때문에 다수의 CA가 존재할 수 밖에 없다. CA의 인증 구조에는 계층 구조와 네트워크 구조, 두 가지가 있다.

2.5.2 계층 구조

계층구조는 다음 <그림 1>과 같이 최상위의 루트 CA가 존재하고 그 아래에 하위의 CA가 계층적으로 존재하는 트리 형태로 상위 인증기관이 하위 인증기관에게 CA 인증서를 발행하며 하위 인증기관은 상위 인증기관의 인증정책에 영향을 받는다(김철, 1996).

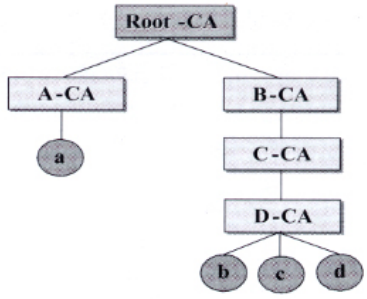

그림 1. 계층 구조.

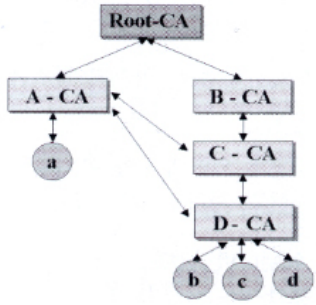

그림 2. 네트워크 구조.

2.5.3 네트워크 구조

네트워크 구조는 상위 인증기관의 영향이 없이 인증기관 각각이 자신이 인증정책에 따라 독립적으로 존재한다. 그리고 필요시 CA 간에 상호인증서를 발행하여 인증서비스를 한다. 위의 <그림 2>는 네트워크 구조를 나타내고 양방향의 화살표는 상호인증 관계를 나타낸다.

2.6 CA의 관리 대상

2.6.1 X.509 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다. 인증서의 형식은 1988년 발표된 X.509 형식을 사용하며 현재까지 X.509 버전 3까지 공표되었다. X.509v3의 형식은 <표 3>과 같다(Greene,1997; 김철, 1996).

2.6.2 X.509 인증서 취소목록(CRL : Certificate Revocation List)

인증서는 인증기관에 의해 설정된 유효기간에 취소 될 수 있다. 그 이유는 다음과 같은 경우가 있다.

- 사용자가 가진 비밀 키의 노출
- 사용자의 무효화 요구
- 사용자의 가입 변경
- 사용자의 소멸
- 사용자의 잘못된 식별
- CA의 비밀키의 노출
- CA의 소멸

표 3. X.509v3 인증 구조

version	X.509의 버전으로 0은 버전1, 1은 버전2, 2는 버전3을 의미함
serial number	발행자가 생성한 각각의 확인서에 대한 유일 식별자
signature algorithm id	발행자가 확인서를 서명하는 데에 사용한 알고리듬을 기입
issuer name	확인서를 서명하고 생성한 발행자의 ID로 X.500 명명 방식을 따름
validity period	확인서가 사용될 수 있는 시작 시간과 끝 시간을 기입하는 것으로 시간과 날짜로 표현됨
subject name	확인서를 받는 공개키의 소유주의 ID로 X.500 명명 방식을 따름
subject public key info	사용자의 공개키와 공개키에 대한 정보(알고리듬과 파라미터)를 기입
issuer unique identifier	(선택) 버전2 이상에서 사용되는 것으로 발행자의 부가적인 정보를 포함함
subject unique identifier	(선택) 버전2 이상에서 사용되는 것으로 객체의 부가적인 정보를 포함함
extensions	(선택) 인증정책 등 여러 가지 사항을 포함함
signature	앞의 목록들에 대한 서명값

인증기관은 유효기간 내에 효력이 상실된 인증서에 대해 CRL을 생성해서 디렉토리에 보관하며 상대편의 인증서가 의심이 갈 때 그 목록을 확인할 수 있다.

CRL 양식은 X.509v2 CRL을 주로 사용하며 다음 표와 같은 형식을 따른다. 인증서 취소목록은 X.509v2 형식을 따르는 추세로 다음 <표 4>와 같다(Greene,1997; 김철, 1996).

표 4. X.509v2 CRL 구조

이 름		설 명	
signature	Algorithm Identifier	CRL을 서명할 알고리듬	
	Parameters	필요한 파라미터들	
Issuer		CRL 발행자 이름으로 X.500 명명 방식을 따름	
this date	UTCTime	갱신일에 대한 타임 스탬프	
next date	UTCTime	다음 갱신일	
revoked certificates		Serial number	취소된 인증서의 일련번호
		revocation date	인증서 취소일
		CRL entry extension (선택)	취소 이유 등 부가적인 정보를 기술함
CRL extenstion(선택)		부가적인 정보를 선택적으로 기술함	
Issuer's signature		발급자의 전자서명	

2.6.3 상호 인증서 쌍(cross-certification pair)

- 순방(forward) 인증서 : 인증기관에 대해 다른 인증기관에서 생성한 인증서
- 역방(reverse) 인증서 : 인증기관이 다른 인증기관에게 생성한 인증서

상호 인증서를 사용함으로써 같은 도메인 내에서는 인증 경로를 단축시키고 다른 도메인 내의 사용자들에게는 안전한 통신 수단을 제공한다.

2.6.4 CA의 인증서 검증절차

인증서를 검증하기 위해서 다음 <그림 3>과 같이 송신자와 같은 CA에 소속되어 있는 경우에 수신자인 사용자 1은 송신자인 사용자 2가 소속된 CA 공개키를 이용하여 서명을 확인한다. 그리고 서명이 유효하면 다음으로 CA의 디렉토리에서 인증서 폐지목록을 다운로드 받아 폐지된 인증서가 존재하는지 여부를 확인하고 있으면 유효하지 않고 없으면 유효한 것이 된다.

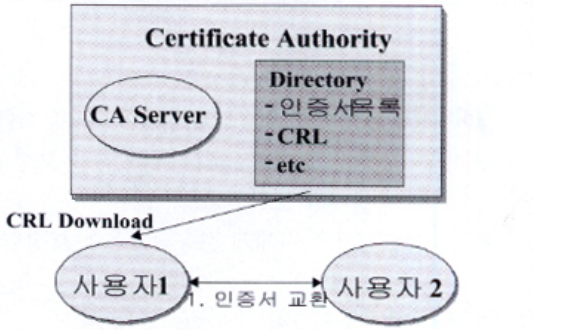

그림 3. 인증서 검증 절차.

3. CITIS

3.1 CITIS 기본 개념

CITIS는 정부가 계약에 의거 요구하는 정보에 대한 전자적인 접근을 제공하고, 전자적인 매체로 납품이 가능하도록 계약자는 정보를 개발 및 유지하는 서비스이다. CITIS는 보통 주계약자를 통해 획득하지만, 주계약자는 관련 하청업체로부터 정보통신망을 사용한다. 따라서 주계약자는 특정 프로젝트에서 정보의 통합자가 된다.

CITIS는 계약자가 생산하는 계약자료요구목록(CDRL)에 대

해 정부기관이 접근할 시, 단일 창구를 통하여 CALS 목표를 달성하며, 자료를 한 번 생산하고 여러 번 활용하고자 하는 것이다. 또한 "정보공유"라는 CALS 개념을 가속화하는 핵심기능이며, 다양한 사용자들이 활용할 수 있도록 데이터의 특성을 표준화한다(한지훈 외, 1999; 홍승필, 1998).

3.2 CITIS 기능 및 범위

CITIS는 계약자간 계약수행에 필요한 기술정보를 전자적으로 전송하는 것을 뜻하기 때문에, 그 적용 범위가 산업 부문 및 계약 당사자간의 합의에 의하여 달라질 수 있는데, 본 논문에서 CITIS의 범위를 잡으면 그 내용은 다음과 같다.

- 조달자와 계약자 사이에 CAD 정보가 upload/download 되게 하며, upload CAD 정보를 축소하여 볼 수 있으며 전송된 정보를 인정/불인정 또는 수정을 요구할 수 있는 설계정보 전자결재
- 조달자가 입찰을 원할 경우 입찰자들이 관련 정보들을 download하여 입찰에 할 수 있도록 하는 공개 입찰지원 시스템
- 조달자는 계약자가 계약을 제대로 잘 준수(수행)하고 있는지 프로젝트 진도 및 지출된 비용을 점검하기 원하기 때문에 프로젝트 진도 관리 및 예산관리를 위한 시스템
- 프로젝트 수행 중 사용자의 DB에 대한 접근 권한, CAD 데이터의 갱신 등 여러 가지 변화가 있을 수 있는데 이러한 변화를 관리하기 위한 변경관리 시스템
- 조달자와 계약자간 의사 소통을 돕기 위해서 게시판 및 help 기능이 있는 대화지원 시스템
- 사용자가 데이터를 접근하려고 할 경우 각 파일(주로 CAD 데이터)에 대하여 사용자 별로 접근 권한을 주어 접근 가능한 역할만 수행하게 하는 DB 접근제어 시스템
- 고가의 정보(CAD 데이터)가 시일이 흘러 개방될 경우, 개방된 파일들을 수요자에게 공급하여 부가가치 수입을 올리는 개방 데이터 관리 시스템
- CITIS는 고가의 정보를 다루고 있으므로 보안이 아주 중요한데 DB 접근제어 시스템이 CITIS 서버 내에서 보안을 책임진다면, 데이터가 서버 밖으로 나와서 인터넷상에서 해킹되지 않도록 SSL(Secure Socket Layer) 설치

<그림 4>는 위에서 설명한 CITIS의 기능 및 범위를 나타낸 것이다. <그림 5>는 CITIS의 기능을 구현하였을 때 가질 수 있는 CITIS의 세부 모듈을 나타낸 것이다.

4. 사용자 인증 시스템 구현

4.1 개발 시스템 환경

CITIS 사용자 인증 시스템 구현을 위한 환경은 다음과 같다.

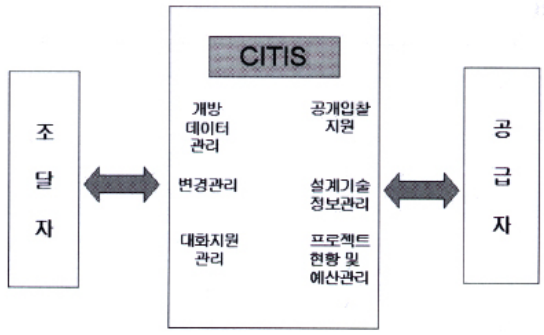

그림 4. CITIS 개념도.

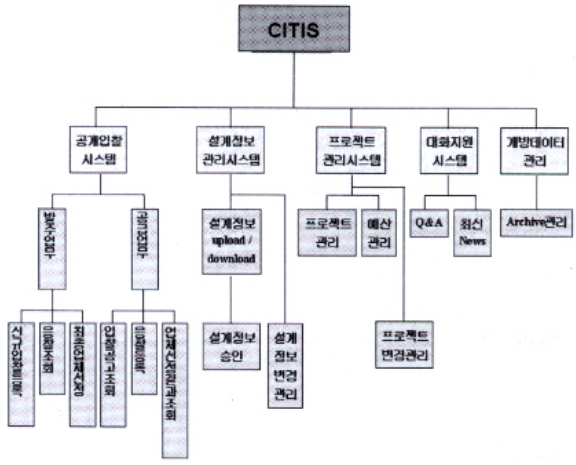

그림 5. CITIS 구조도.

- 운영체제 : Microsoft Windows NT 4.0
  (Service Pack 3, Option Pack 4)
- 웹 개발 도구 : Active Server Page
- 데이터베이스 : MS-SQL6.5
- 웹 서버 : Internet Information Server
- 암호시스템 : Microsoft Cryptography Service Provider 2.0

4.2 사용자 인증 시스템 데이터 구조

CITIS 사용자 인증을 위한 인증서 요청, 취소목록, 기타 공개키 정보 등록을 위한 시스템의 데이터베이스 정보는 다음 <표 5>에서 <표 8>과 같이 구성된다.

4.3 사용자 인증 시스템

4.3.1 사용자 인증 시스템 개요

CITIS 사용자 인증 시스템은 크게 세 부분으로 나눌 수 있다.

가. CITIS 서버 인증

나. CITIS 클라이언트 인증서 발급

다. 인증서를 통한 CITIS 사용자 확인(안전한 통신)

표 5. CRL 테이블

Field 명	Data Type	내 용
RevocationID	number	Revocation List의 ID
IsserNameID	Number	발생자의 ID
Issued	Data/Time	List가 발행된 날짜
Next	Date/Time	다음 List가 언제 생성될 것인가?

표 6. Requests 테이블

Field 명	Data Type	내 용
RequestID	number	요청서 ID
RequestType	number	요청서 타입
RequestStatus	number	요청서 현재 상태
SubmittedWhen	Date/Time	제출된 날짜/시간
ResolvedWhen	Date/Time	승인되거나 거부된 날짜/시간
RevokedWhen	Date/Time	취소된 날짜/시간
RevokedEffectiveWhen	Date/Time	취소효력 날짜/시간
RevokedReason	number	취소 이유
RequesterName	string	요청자 이름
RequestAddress	string	요청서의machine/ network / email 등 기타 정보

표 7. Certificates 테이블

Field 명	Data Type	내 용
RequestID	number	인증서 ID
CertificateHash	string	인증서 해쉬 함수
CertificateType	number	인증서 타입
SerialNumber	string	인증서 일련번호
IssuerNameID	number	발행자 ID
SubjectNameID	number	Subject ID
NotBefore	Date/Time	유효기간 시작
NotAfter	Date/Time	유효가간 끝
PublicKeyAlgorithm	string	Public Key 알고리듬

표 8. Names 테이블

Field 명	Data Type	내용
NameID	number	필드 ID
NameType	number	Name Type
Country	string	사용자 정보
Organization	string	사용자 정보
OrganizationalUnit	string	사용자 정보
CommonName	string	사용자 정보
Locality	string	사용자 정보
StateOrProvince	string	사용자 정보
Title	string	사용자 정보
GivenName	string	사용자 정보
Initials	string	사용자 정보
SurName	string	사용자 정보
DomainComponent	string	사용자 정보
EMail	string	사용자 정보
StreetAddress	string	사용자 정보

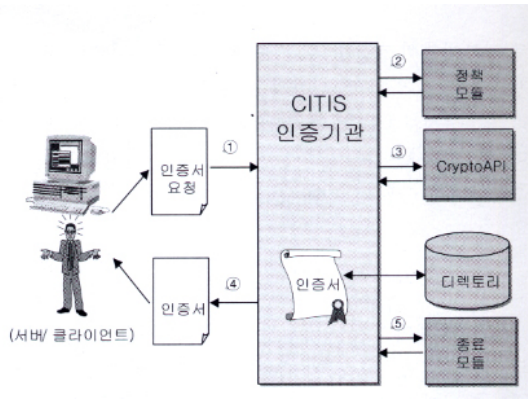

그림 6. 사용자(서버/클라이언트) 인증서 발급.

<그림 6>은 CITIS 사용자 인증 시스템 부분 중 "가", "나" 즉 CITIS 인증기관이 CITIS 서버와 CITIS 사용자(클라이언트)에게 인증서를 발급하는 과정을 설명한 것이다.

1. 인증서 요청
   ▶ ASP를 통해서 처리
2. 정책 모듈(policy module)을 이용해서 요청 실행
   ▶ 정책 모듈 : 인증서를 발행하기 전에 인증 기관이 필요로 하는 정책을 구현하는 객체
   ▶ 정책의 예
   - X.500 Field Name을 무조건 회사이름으로 한다.
   - 특정 지역에 사는 사용자의 인증서만 받아들인다.
   ▶ 인증서 요청외에 다른 기타 정보를 처리 한다.
   -요청자의 전화번호, 주소, 주민등록번호 등을 요구할 수 있다.
3. 인증서 생성
   ▶ CryptoAPI(Cryptography Application Programming Interface)를 사용
   ▶ 인증서에 CA의 비밀키로 Digital Signature를 추가
   ▶ CryptoAPI
   - 암호화 서비스 제공자 역할
   - 데이터 처리, 서명, 공개키/비밀키 쌍을 저장하는 역할
   ▶ 인증서 요청 정보와 인증서 정보를 디렉토리에 저장
   - CRL를 생성하기 위한 정보.
4. 인증서 발행
   ▶ 요청한 정보를 토대로 Cryptosystem Provider가 인증서를 생성하여 사용자에게 발행한다.
5. 종료 모듈
   ▶ 인증서 요청 처리과정 종료

CITIS 서버와 클라이언트의 인증서 요청 처리과정이 끝나면 CITIS 서버는 사용자의 인증서를 확인함으로써 안전한 통신을 수행할 수 있다. <그림 7>은 CITIS 사용자 인증 시스템중 "다" 부분인 인증서를 통한 사용자 확인을 나타낸 것이다. CITIS 사용자가 CITIS 서버에게 접속을 요구하면 CITIS 서버는 사

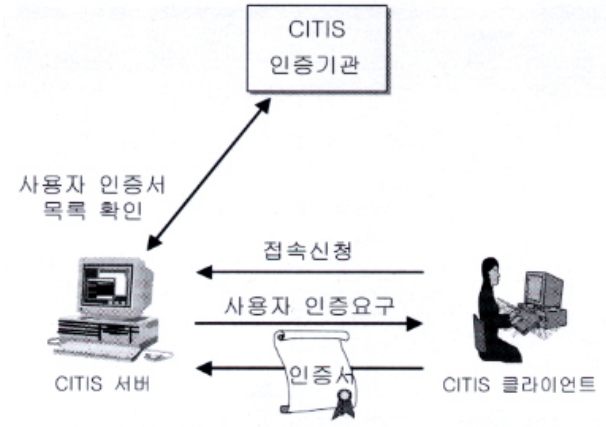

그림 7. 인증서를 통한 사용자 확인.

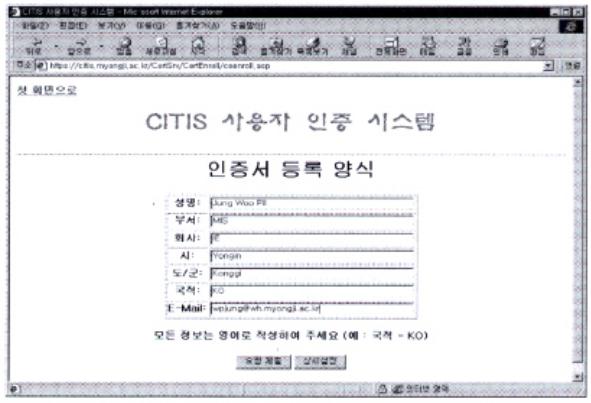

그림 9. 사용자 인증서 요청 양식.

용자 인증을 요구하게 된다. CITIS 사용자는 CITIS 서버에게 CITIS 인증기관에서 받은 인증서를 브라우저를 통해서 제출함으로써 자신을 확인시켜준다. CITIS 서버는 사용자 인증서가 유효한지를 확인한다. 유효하면 안전한 통신을 할 수 있는 환경이 된다.

4.3.2 사용자 인증서 발행

<그림 8>부터 <그림 11>에 보여지는 화면들은 CITIS 인증기관에게 사용자가 인증서를 요청하고 그것을 인증기관이 처리하는 과정을 나타낸 것이다. 사용자 인증서 요청을 하기 위해서는 CITIS 인증기관의 메뉴 중에서 사용자 인증서 요청을 통하여 처리한다.

1. CITIS 인증 시스템 초기 화면

<그림 8>은 본 논문에서 구현한 CITIS 사용자 인증 시스템 초기 화면이다. CITIS 사용자 인증 시스템은 인증기관 인증서 설치하기, Web 서버 인증받기, 사용자 인증서 요청 등 세 부분으로 구성되어 있다.

2. 사용자 인증서 요청 양식 전송

<그림 9>는 "사용자 인증서 요청" 모듈을 나타낸 것이다. CITIS 서버를 사용하기 위해 CITIS 사용자는 먼저 CITIS 사용자

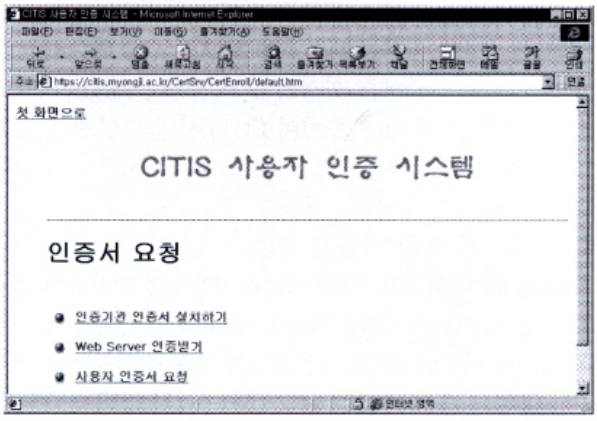

그림 8. CITIS 사용자 인증 시스템 초기화면.

인증기관으로부터 사용자 정보를 등록하고 그것을 요청함으로써 사용자 인증서를 받을 수 있다.

3. 사용자 인증서 상세 설정

<그림 10>은 "사용자 인증서 요청" 모듈 중에서 옵션을 처리하는 부분이다. 사용자는 이 화면을 통해서 인증서의 사용 목적, 암호 알고리듬 등의 옵션을 지정할 수 있다.

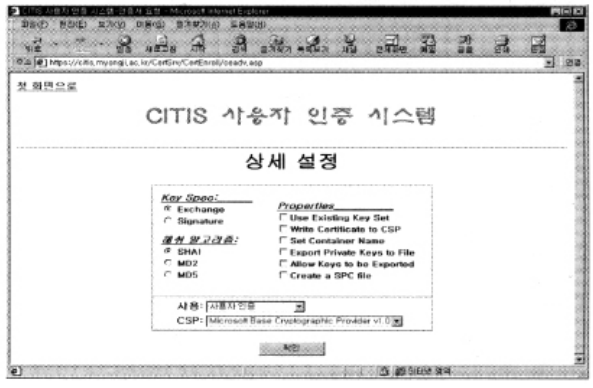

그림 10. 사용자 인증서 요청 상세 설정.

<그림 11>은 사용자 인증서 요청이 CITIS 사용자 인증 기관에 의해서 처리되었음을 나타내는 화면이다. CITIS 인증기관이 인증 정책에 의해서 인증 요청을 승인하면 사용자는 CITIS 인증기관의 인증서를 다운로드할 수 있다. 다운로드된 인증서를 CITIS 서버에게 자신을 확인할 수 있는 수단으로 사용된다.

4.3.3 서버 인증서 발행

<그림 12>부터 <그림 17>의 화면들은 CITIS 서버가 CITIS 인증기관에게 인증서를 요청하고 그것을 인증기관이 처리하는 과정을 나타낸 것이다. 웹 서버 인증서 요청을 하기 위해서는 CITIS 인증기관의 메뉴 중에서 웹 서버 인증 받기를 통하여 처리한다.

1. 서버 인증 요청 파일 생성

<그림 12>는 CITIS 인증기관에게 CITIS 서버 인증서 요청

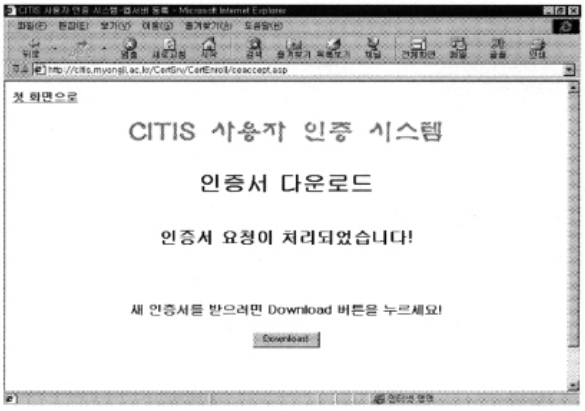

그림 11. 사용자 인증서 요청 처리.

그림 12. CITIS 서버 인증 요청 파일.

을 위한 인증 요청 파일의 내용을 나타낸 것이다. CITIS 서버의 정보를 암호화된 내용으로 바꾸어서 서버 인증 요청 파일을 생성한다. 생성된 인증 요청 파일의 내용 중에서 BEGIN NEW CERTIFICATE REQUEST~END NEW CERTIFICATE REQUEST 부분의 내용을 Web 서버 인증을 위하여 사용한다.

2. 서버 인증서 요청

<그림 13>은 CITIS 서버에서 생성한 인증 요청 파일의 내용을 CITIS 인증기관에게 제출하는 과정을 나타낸 것이다. CITIS 인증기관은 CITIS 서버에서 제출한 내용을 검토한 후 인증 정책에 의거하여 CITIS 서버를 인증하게 된다. 인증 요청이 처리되면 CITIS 서버는 CITIS 인증기관으로부터 인증서를 다운로드 할 수 있게 된다.

3. 서버 인증 요청 처리

<그림 14>는 CITIS 서버가 요청한 Web 서버 인증서 요청을 CITIS 인증기관이 처리한 결과를 나타낸 화면이다. CITIS 서버는 CITIS 인증기관으로부터 다운로드한 인증서를 사용하여 사용자 인증을 위한 안전한 통신 환경을 구성할 수 있게 되고, 또한 인증서를 사용하여 CITIS 서버 자신도 안전한 사용자임을 입증할 수 있게 된다.

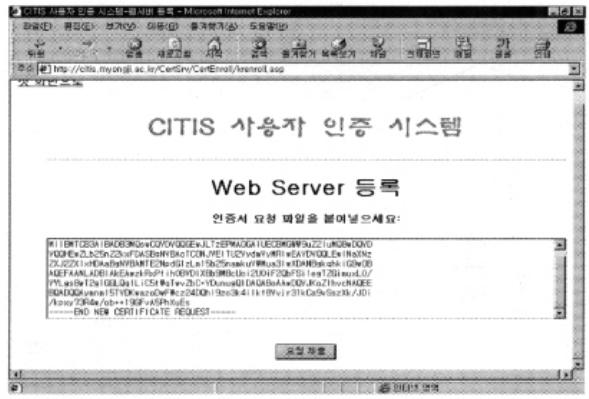

그림 13. CITIS 서버 인증서 요청.

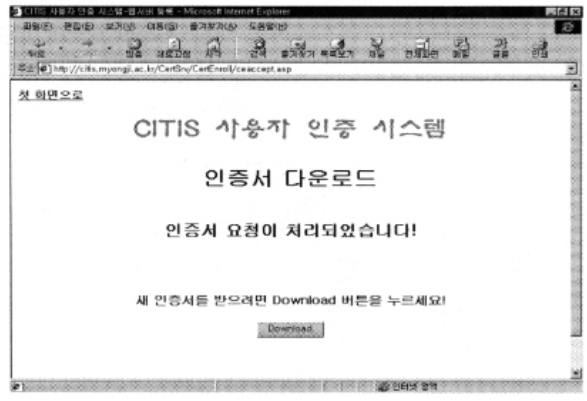

그림 14. CITIS 서버 인증서 요청 처리.

4.3.4 CITIS 사용자 인증

CITIS 서버와 사용자는 CITIS 인증기관으로부터 받은 인증서를 통하여 서로를 확인할 수 있다. 즉, CITIS 서버는 사용자 인증을 할 수 있게 되고, 그럼으로써 안전한 통신을 할 수 있게 된다. <그림 15>부터 <그림 17>은 CITIS 인증기관으로부터 받은 인증서를 가지고 CITIS 서버와 CITIS 사용자가 서로를 인증하고 안전한 통신의 환경을 구성하는 내용을 나타낸 것이다.

1. 사용자의 CITIS 서버 확인

<그림 15>는 CITIS 사용자가 CITIS 서버에 접속하였을 때 CITIS 서버의 인증서를 확인하는 화면이다. CITIS 사용자는 CITIS 서버의 인증서를 통하여 CITIS 서버의 안전성을 확인한다.

2. 인증서를 통한 사용자 확인

<그림 16>은 CITIS 서버가 CITIS 사용자에게 사용자 인증을 요청하는 화면이다. CITIS 사용자가 CITIS 서버에 접속을 시도하면 CITIS 서버는 CITIS 사용자에게 사용자 인증을 요청하게 된다. CITIS 사용자는 브라우저에 있는 자신의 인증서를 CITIS 서버에게 확인시켜 줌으로써 사용자 인증을 할 수 있다.

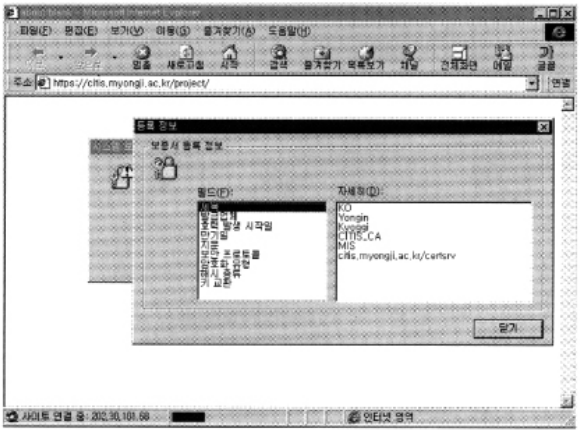

그림 15. 사용자의 CITIS 서버 인증서 확인.

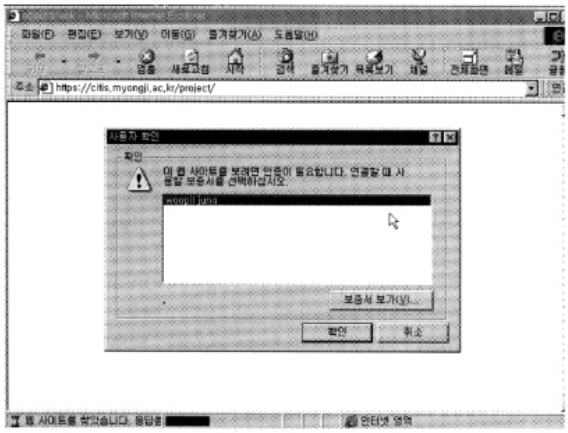

그림 16. 인증서를 통한 사용자 확인.

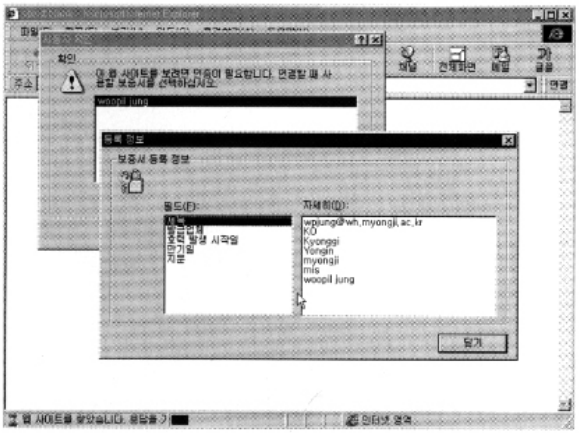

그림 17. 사용자 인증서 정보.

3. 사용자 인증서 정보

<그림 17>은 CITIS 사용자 인증서의 정보를 나타낸 화면이다. 사용자 인증서의 내용은 CITIS 인증기관에게 인증서 요청할 때 등록한 사용자 정보와 CITIS 인증기관의 정보 등이 나타나게 된다.

4.3.5 CITIS 사용자 인증 시스템 구현 결과

<그림 12>부터 <그림 17>에서 CITIS 사용자 인증 시스템의 구현 화면을 보였다. 이상에서 보인바와 같이 CITIS 서버와 CITIS 사용자는 CITIS 인증기관으로부터 인증서를 받아서 그것을 통하여 서로의 신분을 확인한다. 특히 불특정 다수의 CITIS 사용자들은 CITIS 인증기관으로부터 인증서를 받은 인증된 사용자들만이 CITIS 서버를 사용할 수 있게 된다. 그럼으로써 CITIS의 보안문제를 해결할 수 있는 환경이 될 수 있다.

5. 결론 및 추후 연구 과제

급속하게 발전하고 있는 전자상거래의 환경을 고려할 때 서로 믿을 수 있는 전자상거래 제공자나 사용자의 확인이 절실히 필요한 때 이다. 특히 전자서명법의 시행으로 인하여 앞으로 전자상거래에서 사용자 인증에 대한 관심은 더욱 고조될 것으로 생각된다. 본 논문에서는 그와 관련하여 안전한 전자상거래를 위한 여러 가지 기술 요소 가운데 가장 기초적인 문제인 사용자 인증과 그와 관련된 기반 기술에 대하여 살펴 보았고 그것을 토대로 CALS의 Data Gateway인 CITIS에서의 사용자 인증을 구현하여 보았다.

사용자 인증 시스템을 구현하면서 상용화된 인증시스템의 접근이 용이하지 않다는 것과 대부분이 아주 고가이며, 쉽게 빌려주는 분위기가 아니라는 것을 발견할 수 있었다. 접근할 수 있는 방법으로 MS 제공 NT기반이 가장 쉽고 보편화되어 있어서 본 논문은 사용자에게 가장 보편화된 환경(Windows NT 사용)에서 CITIS를 구현할 때 어떻게 하는 것이 좋은가를 제시하였다.

사용자 인증 시스템을 구현하기 위하여 공개키 기반구조를 사용하였다. 공개키 기반구조는 인증기관, 등록기관, 사용자, 디렉토리로 구성되어 있는데 본 논문에서는 이러한 구성 요소 중에서도 인증기관의 기능을 활용한 사용자 인증 시스템을 구현하였다. CITIS 인증기관은 목적 시스템인 CITIS 서버와 CITIS 사용자를 인증한다. CITIS 서버는 CITIS 인증기관으로부터 받은 인증서를 가지고 CITIS 사용자를 인증하기 위한 서비스를 구현한다. 즉, CITIS 사용자가 CITIS 서버에 접속을 요구하면, CITIS 서버는 CITIS 사용자에게 사용자 인증을 요청하게 되고, CITIS 사용자는 CITIS 인증기관으로부터 받은 인증서를 브라우저를 통하여 CITIS 서버에게 제출함으로서 자신을 확인시켜준다. CITIS 서버는 CITIS 인증기관으로부터 사용자 목록을 확인함으로써 CITIS 사용자를 인증하게 된다.

이러한 사용자 인증 시스템은 그 자체뿐만 아니라 다른 응용 프로그램 및 전자 상거래 응용 시스템과 통합적인 사용이 중요하다. 따라서 사용자 인증 시스템을 활용한 전자 상거래 서비스에 대한 연구가 진행되어야 할 것이며, 인증 기술을 이용하여 사용자 인증 뿐만 아니라 사용자들이 주고받는 전자적인 Data에 대한 인증도 추후 연구되어야 할 것이다.

참고문헌

김철 (1996. 12), 암호학의 이해, (주)영풍문고.

삼성SDS (1999. 7), 전자인증 솔루션 구축 및 활용 사례, *CALS/EC Korea proceeding*, 2, 677-692.

선우종성 외 3 (1998. 12), 정부 전자문서를 위한 인증 소프트웨어 기능 표준에 관한 연구, 한국전산원.

송용옥 (1999. 6), 인증서 표준 및 인증체계, *한국과학기술원 테크노대학원 전자상거래 연구센터 제2 회 전자상거래 워크샵proceeding*, 9-14.

염용섭 (1998), UN/EDIFACT레벨에서의 정보보호, *한국CALS/EC 학회지*, 3(2), Dec.

이덕형 (1998. 12), 데이터보안과 공개키 기반구조 (PKI), *한국전자거래 (CALS/EC) 학회proceeding*.

이재규 (1999.), 전자상거래 인증체계의 동향, *한국과학기술원 테크노대학원 전자상거래 연구센터 제2회 전자상거래 워크샵proceeding*, 3-7.

전성배 (1999. 9), 전자인증제도, *제1회 정보보호 심포지엄(SIS '99) proceeding*.

정석찬 외 3 (1997), CITIS(Contractor Integrated Technical Information Service) 구현에 관한 고찰, *한국경영과학회/대한산업공학회 '97 춘계공동학술대회*.

최진주 외 1 (1998. 12), 전자상거래에서 인증서 검증 절차 개선방안 연구", *한국전자거래(CALS /EC) 학회proceeding*.

하경주 외 3 (1999. 3), 보안토큰을 이용한 웹 보안 시스템 개발, *한국정보처리학회 논문지*, 6(3).

한국증권전산(주) 전산기술연구소 (1998. 11), 한국증권전산 인증기관 인증실무 준칙".

한지훈 외 7 (1999. 1), 공개키를 이용한 SNMPv3 보안 모듈 설계 및 구현, *한국정보처리학 회 논문지*, 6(1).

홍승필 외 1 (1998. 5), 정보보안 기술과 구현, 파워 북.

Ahuja. Vijay(1997), Secure Commerce on the Internet, *AP Professional*.

Cericom, Cryptography Technology : *http://www.certicom.ca*

DoD (1993), MIL-STD-974: Contractor Integrated Technical Information Service(CITIS), *Department of Defense, U.S.A*.

Greene. Mark. (1997. 5), Role of Certificate Authority in Internet Commerce.

IETF Draft (1998), Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

IETF Draft (1998), Internet X.509 Public Key Infrastructure Certificate Management Protocols.

ISO/IEC (1992), CCITT X.500, The Directory : Overview of Concepts, Models and Services, CCITT.

NIST (1994), The 1994 Mitre PKI Study Final Report, *http://csrc.ncsl.nist. gov/pki/mitre.ps*.

Rosing (1999). Michael, Implementing Elliptic Curve Cryptography, Manning.