通信情報保護學會誌
第8卷 第3號, 1998. 9

CA 시스템 적용 모델 및 현황

안 혜 연*

요 약

최근 정보 보안 및 전자 상거래 관련된 영역에서 certificate (인증), certificate authority (인증기관) 및 Public Key Infrastructure (공개키 기반 구조) 등에 대한 관심이 고조되고 있다.

이러한 기술은 보안의 기본 요소인 인증(authentication), 기밀성 (confidentiality), 무결성 (Integrity) 및 부인봉쇄(non-repudiation) 등의 기능을 커다란 규모의 시스템에 적용할 수 있는 거의 유일한 solution이 될 것이 확실하다. 이 자료에서는 CA(Certificate Authority) 관련 기술 자체에 대한 자세한 설명보다는 개념적인 차원에서의 소개와 적용 영역 및 적용 model에 대해 소개하였다

1. CA 시스템 소개

CA 시스템이라는 것이 아직은 일반인들에게 상당히 낯설고 새로운 개념이므로 먼저 certificate 자체에 대한 개념과 Certificate Authority(CA)의 role에 대해 간단히 소개 하였다. 또한 이것들이 사용되는 전체적인 적용 환경인 Public Key Infrastructure(PKI)에 대한 개념 및 구조에 대해 자세히 언급하였다. 여기서 CA 시스템이라 함은 CA 서버를 주축으로 구축된 PKI 환경을 의미한다.

1.1 Certificate란 ?

우리가 중요한 거래를 할 때 흔히 계약 서류에 날인을 하고 인감증명서를 첨부한다. 컴퓨터 네트워크 통신의 경우도 마찬가지로 호스트, 개인, 프로그래머 등이 자기 자신임을 증명하려면 각자 도장을 하나씩 가지고 있어야 하며 CA에 인감 등록을 해야 한다. Certificate Authority(공증사무소)는 신청된 도장에 대해 본인확인을 한 후 인감 등록을 하고 certificate(증명서)를 발급 하며, 실제 안전하게 보호된 컴퓨터 통신이 시작될 때 호스트간 혹은 개인간에 certificate(증명서)를 제출, 교환 함으로서 상대를 확인 한다

동사무소에서 발급하는 인감증명서도 양식이 있듯이 전자적으로 사용하는 증명서에도 형식이 있는데 여기서 발급하는 증명서는 X.509 certificate라는 양식을 사용 한다. 공개키 기반구조에서 도장의 역할을 하는 것이 public key로 CA가 public key를 증명하는 certificate

*삼성 SDS

를 발급할 때 단순히 public key에 전자서명만 해주는 것이 아니라 public key의 소유주와 public key의 알고리즘, 서명자, 서명방식 등을 포함하며, 이것들을 부호화 하는 일반적인 방법이 통신 표준 제정 기관인 ITU-T에서 제안한 X.509 certificate 형식 이다.

1.2 Certificate Authority

Certificate Authority는 위에서 설명한 public-key Digital ID인 Certificate를 발행하고, 갱신하고, 폐기하며 이러한 기능을 수행하기 위한 인증 절차를 정립하고 관리한다. 이러한 Certificate Authority는 기본적으로 business-to-business 경우와 일반을 대상으로 하는 전자 상거래에서의 보안 기능을 개선하고 또한 기업 내부에 있어서의 접근 제어와 여러 application들을 위한 Single-sign-on 기능을 구현하기 위해서 존재하게 되었다. 기본적으로 Certificate Authority는 공정하게 운영되는 제3자에 의해서 행해지거나 국부적인 관리를 위해 기업내부에서 자체적으로 운영될 수 있다.

이렇게 운영되는 Certificate Authority는 certificate policy를 수립해야 하는데 certificate policy는 X.509 certificate를 이용한 공개키 기반구조(PKI)를 구축하여 운영하고자 할 때 사용자 및 운영자가 지켜야 할 보안 정책인 것이다 사용자들은 certificate policy에 정의된 certificate 신청 절차 및 획득 방법, CA로 부터 발급 받은 certificate의 사용 범위, certificate 폐기 및 재발급 절차, 암호화 및 전자서명 key의 관리, 개인의 보안 통제 기준 등을 숙지하고 이해 하여야 이에 따른 권한과 책임을 올바르게 수행할 수 있다. 마찬가지로 CA 관리자(PKI 관리자)들은 certificate policy를 통해 certificate의 발급에 필요한 사용자의 식별과 Key의 생성, 보증 등급의 부여, 확장 필드의 정의, certificate 폐기의 처리, certificate와 CRL의 디렉토리 공표와 보관, 재해 복구, policy의 관리, 물리적/기술적 보안 통제의 기준 등을 숙지하고 이해 하여야 한다.

이러한 CA 서비스 시 certificate 발급자 또는 certificate 사용자들에 대한 권리와 책임, 의무 등에 대해서 구체적으로 언급되어져 있어야 하며 일반인을 대상으로 하는 공중 서비스인 경우 법적인 효력을 갖도록 되어 있어야 한다.

현재 형성되고 있는 Certificate Authority 관련된 market 영역를 보면 크게 세 부분으로 구분되어 진다. 먼저 CA service를 제공하는 기관으로 이 기관은 원하는 사용자에게 certificate를 발급해 주므로써 사용자가 그 certificate를 사용할 수 있도록 한다. 이 경우 기업 사용자들에게는 outsourcing service 형태가 될 것이며 개인 고객을 위한 public service 형태가 될 수도 있다.

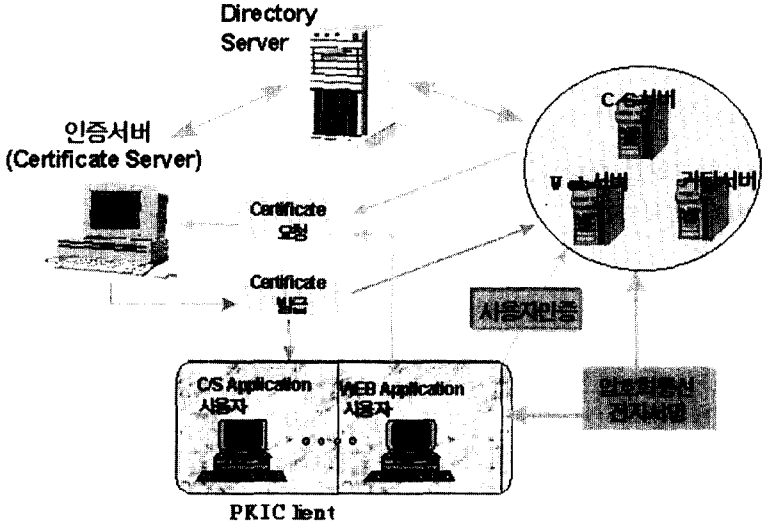
또 다른 영역은 CA system 과 tool에 대한 solution 제품 영역이다. CA system solution 업체의 경우 고객은 public service를 행하는 업체는 물론 내부적으로 CA를 구축하여 사용하는 고객이 주요 대상이 될 것이며 tool solution은 CA 시스템을 자체 구현 할 수 있는 tool을 제공하는 것이다.

1.3 PKI 기술 구조

지금까지 certificate와 Certificate Authority에 대해서 알아보았는데 실제 이것이 적용되어 사용되는 상황인 PKI(Public Key Infrastructure)에 대해서 설명하고 관계를 알아 보겠다. Public Key Infrastructure는 공개키를 기반으로 하는 certificate 배달 시스템으로 certificate request와 key쌍의 생성, certificate의 발급 및 수용, 암호화/전자서명

key관리, 사용자 관리, 각종 ceritificate의 정보의 저장 및 제공 등 다양한 기능을 지원한다. 즉, PKI는 특정 application들이나 system 환경에서 기본적인 암호 관련 서비스를 제공하기 위한 기반 구조로서 certificate를 이용한 사용자 인증 및 안전한 네트워크의 구성은 물론, private key와 public key 쌍을 이용한 전자사명 및 암호화를 지원한다.

PKI의 구성 요소는 certificate 발급, 관리하는 CA(Certificate Authority), certificate 및 CRL을 공표하고 사용자 정보를 제공하는 보관소(Directory Server), 사용자가 PKI환경을 사용하기위한 PKI Client module 등으로 구성 되며 이 세 요소간의 관계는 다음 그림과 같다.



1.3.1 Certificate Authority(CA)

CA는 PKI의 핵심 구성 요소로 사용자을 위한 certificate를 발급, 발급된 certificate의 폐기 및 재발급, 보관소로의 공표, 사용자의 암호화 key의 생성 및 Key escrow, certificate policy의 관리, 각종 정보의 Log/Audit등의 기능을 수행 한다

주요 기능

- ○ Key 관리
  - CA 마스터 key 생성
  - 전자서명 key의 중복 check, 사용자 암호화 key의 생성 발급
  - Key escrow 시스템 : 암호화 key생성, Key 백업, 인출
- ○ certificate 관리
  - cetificate 요청 관리
  - certificate 발급 및 보관소 공표 (발급되는 certificate : 전자서명 certificate, 암호화 certificate)
  - certificate 폐기(CRL) 관리
  - cross certificate 관리
- ○ CA 관리
  - CA 관리자 등록 및 삭제
  - certificate policy 관리
  - processor 관리
  - Log/Audit 관리

1.3.2 Directory Server(보관소)

Directory Server는 공개적으로 이용 가능한 데이터베이스의 저장 및 certificate 검색, CRL과 certificate의 보류 및 폐기 정보, 현재와 과거의 certificate policy, 사용자의 패스워드 및

각종 정보등을 제공하며 X.500 표준이 널리 사용되어 진다.

주요 기능

- ○ 사용자 정보 관리
  - 사용자 DN 확정
  - 사용자 등록 정보 입력
  - 디렉토리 서비스 사용자 등록
- ○ Certificate 서버 Interface
  - certificate 공표
  - CRL 공표
  - Policy 공표
  - 만료된 certificate/CRL 삭제
- ○ 디렉토리 서비스 정보 조회
  - 사용자 정보 조회
  - certificate 정보 조회
  - CRL 정보 조회
  - certificate 다운로드 및 설치
  - CRL 다운로드 및 설치

1.3.3 PKI Client

PKI Client는 CA에 의해 발급된 certificate를 사용하여 메세지를 암호화하고 전자서명을 구현하는 사용자 모듈로 최초 Certificate 신청 및 발급된 certificate의 다운로드, 설치, certificate의 폐기 요청 및 보관소에 공표된 암호화 및 전자서명을 위한 상대방의 각종 key의 획득, 사용자 정보의 조회, CRL의 다운로드등이 수행 된다

주요 기능

- ○ Key 관리
  - 사용자 패스워드 변경 및 관리(보관소에 저장)
  - 사용자의 전자서명 및 암호화 key쌍의 관리
  - certificate 신규 발급 및 재발급시 전자서명 key의 생성
- ○ certificate 관리
  - certificate 발급 요청
  - certificate 설치
  - certificate 폐기
- ○ 알고리즘
  - 메세지 구조 생성(PKCS #7 포맷)
  - 메세지 암호화/복호화(대칭키:DES, RC4, RC2, 3-DES, 공개키:RSA)
  - 메세지 전자서명/검증(해쉬알고리즘:SHA-1, MD5, 전자서명:RSA,KCDSA)
- ○ 보관소(디렉토리 시스템) I/F
  - 접속 인증
  - certificate/CRL 설치(다운로드)
  - 사용자 정보 조회
  - Policy 조회

2. CA 시스템이 적용될 주요 영역

인터넷상에서 신용카드를 사용하는 application에는 SET이 적용된 PKI가 구현될 것이며, 정부 기관이나 상업용 환경에서도 application에는 물론 장비나 자료에 해당하는 부분까지의 접근 제어 등을 위해 PKI가 사용될 것이다. 이밖에도 넓은 다른 영역의 시스템들에서도 PKI 시스템이 활용될 것이 틀림없다. 그 대표적인 영역들을 언급해 보면 다음과 같다.

2.1. 금융 부문

다양한 종류의 금융 서비스가 CA를 적용한 PKI 시스템이 적용되는 가장 대표적인 영역이 될 것이며 또한 가장 빨리 적용되는 영역이 될 것이다. 그 이유는 금융관련 거래에서 암호화, 전자서명 및 인증 등에 관한 기능에 대한 요구가 가장 크기 때문이다. 이러한 서비스는 금융기관 내부용일 수도 있고, 금융기관이 관여된 기업간의 업무일 수도 있으며, 고객이 일반인인 상용 서비스일 수도 있다. 즉 모든 경우의 금융 관련 업무들에 적용될 것이다.

표 1. Electronic Transation Set

Transation	내 용	From	To
Certificate	사용자가 CA에 certificate의 발급을 요청	사용자	CA
	전자서명 Certificate sign 및 발급	CA	사용자
	암호화 Certificate sign 및 발급	CA	사용자
	암호화 Key 생성 및 발급	CA	사용자
Certificate	사용자가 certificate 폐기물 요청	사용자	CA
	폐기 확정 및 거부 여부 통보	CA	사용자
Certificate	사용자가 certificate 재발급을 요청	사용자	CA
	Certificate sign 및 발급	CA	사용자
Retrieve Certificate	타 사용자의 Certificate를 요청 검색	사용자	보관소
Retrieve CRL	CRL를 요청 (다운로드)	사용자	보관소
Post Certificate	CA가 보관소에 발급된 Certificate를 공표	CA	보관소
Post CRL	CA가 보관소에 CRL을 공표	CA	보관소

2.2. 정부, 공공 부문

정부, 공공 기관들에서는 여러 목적의 application에서 사용자의 identity를 확인하기 위한 방법으로 인증서의 활용을 적극적으로 검토해야 하며, 일부 적용되고 있다. 일반적으로 certificate가 한번 발급되면 상당히 긴 시간 동안 유용하게 사용될 수있으며 비용도 과다하지 않기 때문에 정부 공공 기관들에서 주관하는 여러 가지 application 서비스에서 널리 받아들여지고 쓰일 것으로 보인다. 그러나 물론 실제 널리 구현, 사용되기 위해서는 검토되어야 할 정책이나 변수들이 많이 있다. 예를 들면, 일반적으로 이러한 적용을 위해 보안성을 고려해서 다양하고 엄격한 정책 및 절차를 만들어 사용하게 되는데 이러한 경우 사용자 입장에서의 불편함 및 실효성이 떨어질 수 있으며, 사용자의 편리함이나 확장성 만을 고려하면 보안상 헛점이 있을 수 있기 때문이다.

2.3. 의료부문

외국의 경우 의료 정보에 대한 보안 요구가 매우 강하며 이러한 민감한 정보를보호하기 위해서 CA 서비스와 PKI 시스템은 대단히 중요한 솔루션이 되고 있다. 그러나 물론 외국에서도 이 영역의 적용이 다른 부분에서보다 빠른 것은 아니다. 그것은 아마 의학 연구 분야 등에 비해 IT 기술 적용에 대한 투자가 느리기 때문일 것이다. 아무튼 이 영역이 PKI의 주요 적용 영역이 될 것이라는 것은 확실하며 국내의 경우도 의료 관련 업무가 점차 시스템화하고 의료 정보의 보안성에 대한 인식이 보편화함에 따라 같은 추세를 보일 것으로 생각된다.

2.4. 국제 및 국내 무역 거래

국제 및 국내에서의 다양한 거래 당사자들 간에 여러 가지 거래 형태가 일어날 경우 거래 내용에 대한 보안 및 인증을 위해 쌍방간의 협의에 의해서 CA 시스템의 활용이 증가

될 것이다. 이러한 적용이 표준화 및 활성화 되어진다면, 편지나 문서 등이 점차 전자적인 방법으로 빠르게 대치되어질 것이다.

2.5. Code Signing

Certificate는 Java applets이나 다른 전자적으로 분배되는 s/w등 s/w application들에 대해서도 발행 사용될 수 있다. 이 기능은 s/w application에 error가 없다거나, 잘 동작을 한다든가 하는 것을 검증해 주는 것이 아니라 s/w code 자체에 대한 근원지를 확인하는 인증 기능 및 그 내용이 변형되었는 지에 대한 검증 기능을 하는 것이다. 이러한 활용은 추후 다양한 형태의 s/w 제품에 대한 판매 등에 매우 유용한 부분이 될 것이다.

3. CA 시스템이 적용 가능한 application 별 분류

3.1. SET 기반의 Secure payment

SET이 적용된 PKI 시스템은 세계적으로 많은 pilot project들이 구현되고 있고, 국내에서도 몇몇 pilot 차원의 project 들이 구현 및 서비스 되어지고 있다. 실제 시스템에 적용되는 속도가 예상보다 느리고 적용 시 문제점들도 논의되고있으나 전자상거래에서의 카드 사용에 대한 부분을 인정한다면 secure한 payment 절차를 위한 적용을 위해 피해갈 수 있을 것 같지는 않다.

3.2. Secure Intranet, Extranet and Electronic Commerce

이 부분의 적용이 실제로 국내에서는 요구가 가장 많고 구현도 많이 진행되고 있다. 그 이유는 최근 Intranet, Extranet 또는 전자상거래 관련 application이 WEB으로 open 되는 경우가 많은데, 모든 경우에 보안 기능이 문제가 되기 때문이다. 이해를 돕기위해 이러한 경우에 해당하는 application 형태의 예를 들면 WEB에서의 증권 거래 시스템, 특정 기업에서 구매 업자들과의 업무를 위한 extranet 구조의 구매 시스템, 기업 내부에서 사용되어지는 workflow application 에서의 전자서명 기능 등을 들 수 있다.

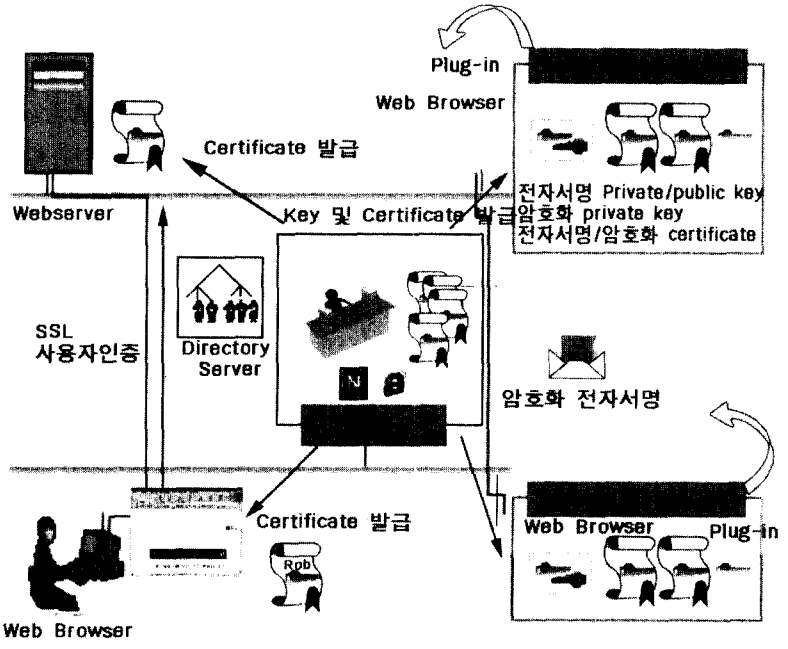
먼저 전자상거래 application을 Internet 상에서 수행하기를 원하는 경우 강력한 인증 기능을 수행하여야 한다. 그런데 Internet 상에서 사용자 인증을 위해 ID/Password를 사용하는 것 보다는 제3자로부터 인증된 증명서를 확인함으로써 각 사용자들에 대한 인증을 하는 것이 보다 강력한 방법이다. 또한 암호화 및 전자서명 기능을 구현할 수 있으므로 사용자가 매우 안전한 Internet business 통신을 원하는 경우 필수적으로 사용해야 할 것이다. 물론 이러한 문제는 매우 작은 규모의 site에서는 중요하지 않을 수 있으나, 대규모의 site에서 많은 수의 거래가 일어나는 경우 심각한 문제로 부각되어진다. 또한 Intranet, Extranet의 경우 이러한 certificate의 활용을 가속화 시키는 몇몇가지 요인을 들자면 다음과 같다.

1. 강한 level의 인증 기능을 원하는 고객들도 특별히 다른 별도의 client 제품을 쓰기보다는 사용하기 쉽고, 쉽게 제공받을 수 있는 browser를 쓰는 것을선호한다.
2. Browser를 제공하는 업체들에서 certificate에 기반한 방법을 채택 구현해 놓았다는 것이 사용자들이 이 방법을 쉽게 적용할 수 있는 요인이 된다.
3. 네트워크를 Internet으로 사용하는 경우 보안상의 문제가 있다는 것이 널리 인지 되었다.

이러한 요인 때문에 기업들이 내부적으로 certificate와 기밀성(confidentiality) 해결에 근거한 높은 보안성을 가지는 Infrastructure를

구현 하려 하고 있다. 중앙관리 하에 쉽게 certificate를 발행하고 폐기하는 기능은 시스템과 application들에 대한 접근제어 관리를 가능하게 한다. Internet을 통해 연결하는 기업간의 application인 경우 이러한 요구는 더욱 중요한 위치를 가진다. 이러한 필요성은 Intranet과 기업간의 Internet 즉 Extranet 경우에 특정 목적을 위한 CA들의 구축을 매우 빠르게 증가시킬것이다.

WEB application을 위해 구축된 CA 시스템 즉 CA에 근거한 PKI의 적용 방법을 그림으로 그려보면 다음과 같다.



CA는 WEB browser와 WEB server에 certificate를 발급하며, WEB browser와 WEB server는 toolkit을 이용하여 구현된 application을 통해 CA와 통신하여 certificate를 발급 받는다. WEB browser와 WEB server는 마찬가지로 toolkit을 이용하여 end-to-end 암호화 통신 및 전자서명 기능을 구현한다.

3.3. VPN

현재 IPSec과 같은 VPN 접근 방법은 사용자를 인증하기 위해서나 네트워크 장비들을 확인하기 위해 인증서 기반에 의존하고 있다. 또한 VPN에서 제공하는 자료에 대한 암호화를 위해서도 PKI를 기반으로 한다. 그러므로 VPN 업체들은 대부분 CA 기술 제공자와 개발 연동 관계를 맺고 있다.

3.4. 인증 및 EDI

기존의 VAN 기반의 EDI 시스템이나 새로운 추세인 Internet EDI 시스템에서도 application의 특성상 상대방에 대한 강력한 인증 및 거래 내용에 대한 암호화, 거래 내용에 대한 무결성 검증 등을 위해 CA 기반의 PKI 솔루션이 반드시 적용되어 져야 하는 부분이다.

3.5. Single sign on

최근 기업 내부에서 각 사용자들이 여러 가지 application들을 사용 하므로써 발생하는 사용자의 번거로움을 줄이고 보안성을 높이기 위해 Single-sign-on 기능에 대한 요구가 많은데 certificate를 사용할 경우 여러 application을 접속하기 위해서 사용되는 password 수를 줄일 수 있다. 이 결과로 각 application의 활용성은 높이고, certificate에 근거한 인증을 하기 때문에 보안성은 강화 되어진다.

3.6. Secure E-mail

E-mail 보안을 위한 S/MIME 표준이나 PGP 를 사용하기 위해 x.509 certificate가 활용되어진다. PKI의 기본 특징 중 하나가 여러 개의 application들을 통합하여 key 관리가 일어날 수 있는 것이므로 위에서 언급한 여러 적용 application들 중 몇몇이 한 site에서 발생할 경우 구축된 PKI가 동시에 여러 application들을 지원하게 된다.

4. EDI 시스템 적용 사례

이 장에서는 3장에서 언급한 여러 경우의 적용 가능 application 중 EDI 시스템적용 경우를 좀 더 상세히 엄급해 보겠다. 먼저 EDI application을 구축하려는 경우 운영시 일어날 수 있는 각 위협 요소를분석하고 그 위협 요소를 해결하는 대책을 수립하며, 그 특성에 적합한 보안 기술을 적용함으로써 안정적인 EDI 시스템을 구축 하여야 한다.

EDI 시스템에서 고려되어야 할 보안 요소는 다음과 같다.

- 기밀성(confidentiality) 보장
- 무결성(Integrity) 보장
- 가용성(Availability) 보장
- 책임 추적성(Accountability) 보장
- 접근제어(Access Control)
- 부인봉쇄(Non-repudiation)
- 감사(Audit)

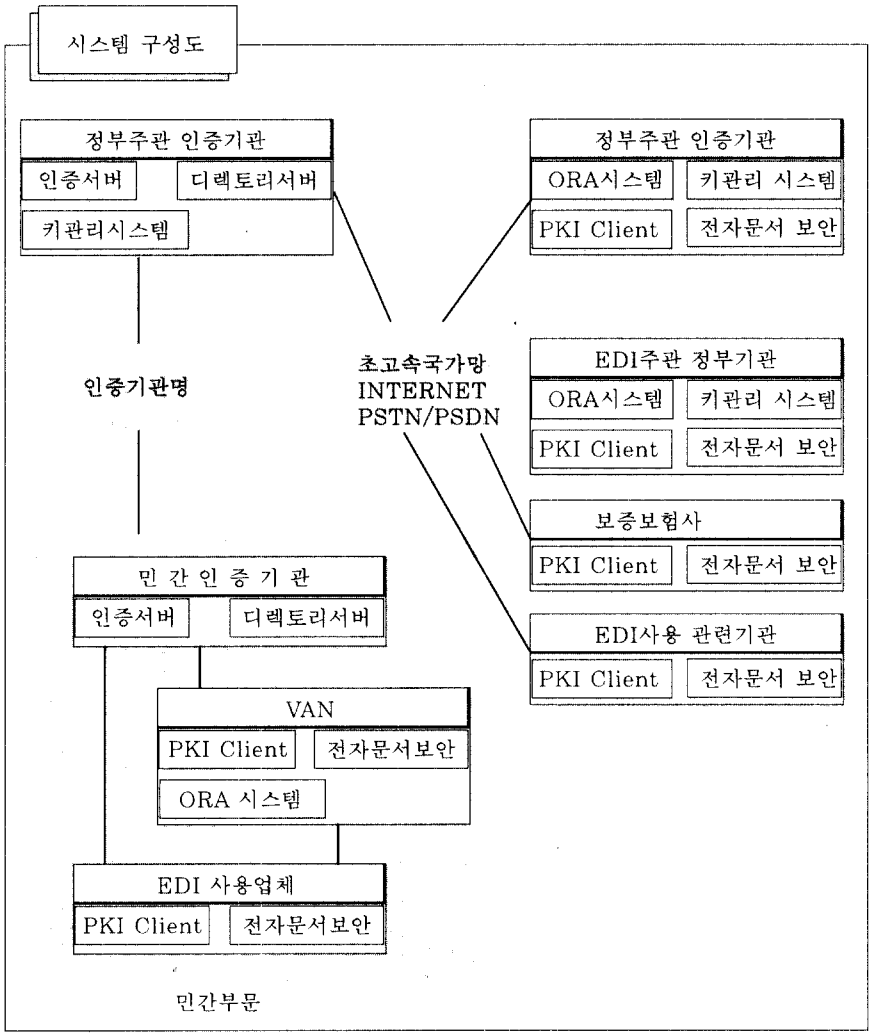
이상과 같은 보안 요소 별로 분석해 볼 때 실제 EDI 시스템에서의 위협 요소를 다음과 같이 생각해 볼 수 있다.

- 전자문서 내용의 불법적인 공개
- 전자문서의 복제, 분실, 중복
- 전자문서 내용의 변조
- 송신자가 전자문서의 송신을 부인
- 불법적인 제3자가 합법적인 송신자로 위장 전자문서 송수신

이러한 위협 요소들은 주로 EDI application에서의 보안상의 문제로 야기될수 있는 문제점들이며, 물론 이 밖에도 네트워크나 서버, 클라이언트시스템들에서도 위협요소를 분석하여 보안 대책을 세워야 한다. 이제 위에서 언급한 위협 요소들, 즉 EDI application에서의 위협 요소들에 대처하기 위한 solution을 검토해 보면 다음과 같다.

- 사용자 접속인증을 강화하여 불법적인 접속 거부
  -Digital Certificate를 이용한 Strong Authentication
- 네트워크상에서 message 내용에 대한 유출 방지
  -EDI message encryption
- 네트워크상에서 불법적인 메시지 변경 검출
  -EDI message에 전자서명 적용 메시지 변조 검출
- 전자서명 및 발신부인봉쇄 구현 법적인 분쟁 위협요소 배제
  -Digital Certificate에 Time Stamp를 적용 발신부인봉쇄 구현

이상과 같이 EDI application에서 CA 시스템을 적용해 보안 기능을 구현하는 방식에 대



한 설명을 하였는데 이제 이러한 구축 및 운영을 위한 시스템 구축 방식을 공공기관에서 주관하는 EDI application의 경우를 들어 검토해 보겠다. 공공기관에서 주관하는 EDI의 경우도 대부분 관련된 공공 기관들과 민간업체들이 연동이 되어지는데 공공 기관을 위한 인증 기관과 민간 부분을 대상으로 하는 인증기관이 분리되어 있을 수 있으며 인증 기관 간에 상호 인증(cross certificate)에 관한 부분이 정립되어 다음 그림과 같이 구현되어져야 한다.

5. 결 론

CA를 기반으로 한 PKI 기술의 구현은 잘 계획되어진 구현 절차나 infrastructure 차원의 투자를 위한 기금, 또한 담당 인력에 대한 교육과 훈련등이 전제되어야 하는 일로, 적용에 대한 필요성도 필수 검토 사항이다.

그러나 이러한 구현의 조건에도 불구하고 지금까지 언급했듯이 놀랄 만큼많은 영역의 application들에서 강력한 인증 등 보안 기능을

위해 구현되어져야 하는 필수적인 솔루션이라는 데는 이견이 없다. 단지 언제 얼마만한 규모로 사용이 될 것이냐 하는 것이 주요 관심사인데 많은 주요 IT trends를 분석 및 예측하는 기관들의 자료 내용과 실제 진행되는 현황을 보면 매우 빠른 속도로 적용되고 있는 것을 알 수 있다.

각 나라별로 입법화나 맨 상위 level의 중앙관리용 CA의 정의 및 설치가 완료되고 있지 않은 상황이나 그 상황 때문에 CA의 국부적인 구축 및 사용이 지연되지는 않는 것 같다. 결국 어떤 분석 보고서의 예측처럼 많은 국부적인 CA의 설치가 상위의 계층 구조를 자연스럽게 형성시켜 나갈 것이라고 생각된다.

장기적인 예측 자료를 보면 2003년 전까지 80% 이상의 기업들이 CA 기술을구현 사용할 것이라고 한다.

□ 著者紹介

안 혜 연

1981 년 2월 이화여자대학교 수학과 졸(학사)
1983 년 2월 이화여자대학교 대학원 전산전공 졸(석사)
1994년 2월 매사츄세츠대 컴퓨터공학과 졸(박사)
1994년 6월 ~ 현재 ; 삼성 SDS 정보기술연구소 재직

※ 주관심분야: