사용자 인증을 위한 공개키 기반구조 시스템 비교·분석

°조한진*, 김봉한*, 이재광*
*한남대학교 컴퓨터공학과

An Analysis and Comparison of Public Key Infrastructure System for User Authentication

°Han-Jin Cho*, Bong-Han Kim*, Jae-Kwang Lee*
*Dept. of Computer Engineering, Hannam University

요 약

공개키 암호시스템은 온라인 전자상거래와 개방형 네트워크에서 정보보호가 요구되는 많은 응용들에 사용되고 있다. 공개키 암호시스템을 광범위하게 사용하려면 공개키 값을 관리하는 공개키 기반구조(Public Key Infrastructure)가 필요하다. 이러한 공개키 기반구조의 기능이 없이, 공개키 암호화는 단지 전통적인 비밀키 암호화와 다를 것이 없다. 본 논문은 전자상거래의 기본이 되는 공개키 기반구조가 기본적으로 갖추어야 할 특징과 공개키 기반구조를 구성하는 객체들, 그리고 공개키 기반구조를 구성하는 기본적인 방법에 대해 살펴보았다. 그리고, 현재 인증 기반 시스템으로 제안·사용되고 있는 PKI 중에서, X.509 기반 시스템(X.509, PEM)과 비-X.509 기반 시스템(PGP, SDSI, SPKI)에 대해 연구를 하였으며, 이에 대해 비교·분석하였다.

Ⅰ. 서론

정보통신 분야의 비약적인 발전으로 인하여 제한적이던 네트워크 환경은 인터넷과 같은 개방된 네트워크 환경으로 변하고 있다. 지금까지 정보의 공유를 목적으로 한 학술·연구용의 인터넷이, 이제는 마케팅을 목적으로 하는 상업용 인터넷으로 바뀌어 가고 있다. 즉, 인터넷 웹서비스를 이용하여 가상공간에서 신용카드나 전자화폐(Electronic Cash)를 이용하여 물건을 구매하고 결제할 수 있는 전자상거래(Electronic Commerce) 서비스가 개발되고 있다.

그러나, 인터넷의 표준 프로토콜인 TCP/IP는 네트워크의 개방성과 소스의 공개로 인하여, 악의(惡意)를 가진 자가 메시지를 가로채어 쉽게 위조할 수 있기 때문에, 인터넷을 사용하는 대다수의 사람들은 보안 문제에 노출되어 있는 실정이다. 따라서, 인터넷을 이용하여 안전한 전자상거래를 구현하려면 보안의 기본 서비스인 접근제어(Access Control),

인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 부인봉쇄(Non-Repudiation) 서비스가 필수적으로 제공되어야 한다. 이러한 정보보호 서비스를 제공하기 위해서 필요한 것이 암호시스템(Cryptosystem)이다.

전자상거래의 안전성과 신뢰성을 확보하기 위해서는, 전자서명의 생성·분배·인증 등에 필요한 절차를 정해야 하고, 네트워크를 통하여 공개키와 인증서를 체계적으로 관리해 주는 기반구조 기술이 필요하다. 전자서명 기술에 사용되는 공개키 암호알고리즘의 비밀키의 기밀성과 공개키의 무결성을 보장하는 것이 공개키 기반구조(PKI : Public Key Infrastructure)이다.

본 논문은 전자상거래의 기본이 되는 공개키 기반구조가 기본적으로 갖추어야 할 특징과 구성 객체들, 그리고 기본적인 구성 방법에 대해 알아보고, 현재 제안된 각 공개키 기반구조 시스템들의 특징에 대하여 연구하였다. 그리고, 공개키 기반구조 시스템이 갖추어야할 특징을 기준으로 해서 공개키 기반구조 시스템들을 비교·분석하였다.

Ⅱ. 공개키 기반구조 개요

공개키 기반구조란 암호시스템과 전자서명 기술을 좀더 체계적이고 조직적으로 관리하기 위해 필요한 기술의 총칭이다. 다시 말해서, 네트워크상에 연결된 각 사용자와 메시지에 대한 인증 기능을 부여하기 위하여, 공개키 방식을 이용한 인증 기반구조이다[1][10].

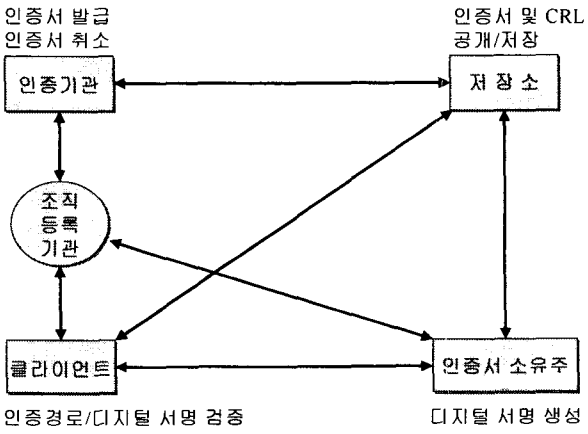
1. 기본 특징

공개키 기반구조의 가장 기본이 되는 기능은 인증(certification)과 검증(verification)이다. 인증이란 개인 또는 조직에게 허가나 자격과 같은 권한을 인정해주는 과정이며, 검증이란 인증기관에 의해 발급된 인증서를 사용할 때, 인증서 정보가 정당한지를 확인하는 과정이다. 인증서에 포함되는 정보는 바뀔 수 있으므로, 인증서 사용자는 인증서의 정보가 정당한지 확인해야만 한다. 검증 방법에는 온라인 검증과 오프라인 검증이 방법이 있다[1][2].

2. 구성 객체

공개키 기반구조의 구성객체는 인증기관(Certification Authority), 조직 등록기관(Organizational Registration Authority), 인증서 소유주(Certificate holder), 클라이언트(Clients), 그리고 저장소(Repository)로 구성된다. 인증기관은 공개키 기반구조를 구성하는 가장 핵심적인 객체로서, 역할에 따라 계층적으로 구성되며 정책 승인기관(Policy Approving Authority), 정책 인증기관(Policy Certification Authority), 인증기관(Certification Authority)으로 분류된다. 조직 등록기관은 CA를 대신해 사용자의 인증서 신청시, 그들의 신분과 소속을 확인하는 기능을 수행한다. 인증서 소유주는 CA, ORA, 그

리고 클라이언트가 될 수 있다. 클라이언트는 사람, 컴퓨팅 시스템(라우터와 방화벽) 또는 응용일 수도 있다. 클라이언트는 신뢰할 수 있는 CA의 공개키를 통해 전자서명과 인증 경로를 검사한다. 저장소는 공개키 인증서와 사용자 관련정보, 상호인증서 및 인증서 취소 목록을 저장 및 검색하는 장소로서, LDAP(Lightweight Directory Access Protocol)을 이용하여 X.500 디렉토리 서비스를 제공한다. [그림 2-1]은 PKI 구성 객체간의 관계를 나타내고 있다[3][4][13].



[그림 2-1] PKI 구성 객체간의 관계

3. 구성 방법

인증기관의 구성은 계층 구조(Hierarchical Infrastructure), 네트워크 구조(Network Infrastructure), 혼합형 구조(Hybrid Infrastructure)로 분류된다. 계층 구조는 한 개의 루트 인증기관 하위에 계층적으로 연결되며, 네트워크 구조는 일반적인 네트워크 환경에서 근접한 인증기관에 대해 상호인증을 할 수 있는 구조이다. 혼합형 구조는 계층 구조와 네트워크 구조를 혼합한 구조로서, 각 루트 인증기관은 자신의 하위 인증기관을 인증하며 동일 계층에 존재하는 다른 인증기관과 상호인증을 한다[1][3][4].

Ⅲ. 공개키 기반구조 시스템

본 장에서는 현재 인증 기반으로 사용되고 있는 여러 가지 PKI 중에서, X.509 기반의 시스템(X.509, PEM)과 비-X.509 기반의 시스템(PGP, SDSI, SPKI)에 대하여 분석하였다.

1. X.509와 PEM

1988년 X.500 디렉토리 권고안으로 처음 발표된 ITU-T X.509는 표준 인증서 형식을

정의하였다. 1988년 X.509v1이 발표된 이래, 1993년 디렉토리 접근 제어(Directory Access Control)를 지원하는데 사용되는 2개의 필드(발행자와 주체의 고유 식별자)가 추가되어 X.509v2가 발표되었다.

1993년 초 PEM(Privacy Enhanced Mail)은 전자우편 보안에 대한 보안 서비스를 제공하는 인터넷 표준으로 제안되었다([RFC 1421], [RFC 1422], [RFC 1423], [RFC 1424]). PEM의 목적은 인터넷 전자우편에 공개키 암호화를 사용해서 기밀성(Confidentiality), 인증(Authentication), 메시지 무결성 보장(Message Integrity Assurance), 발신처 부인봉쇄(Non-repudiation of Origin)를 제공하는 것이다. PEM은 X.509v1 인증서에 기반한 공개키 기반구조를 위한 규격을 포함하였는데, 이 때 X.509v1 및 X.509v2 인증서를 그대로 수용하기에는 문제점을 가지고 있다. PEM을 설계하고 구현하기 위해서는 정보를 전달할 수 있는 추가적인 필드의 필요성이 제기되어, 이를 해결하기 위해 ISO/IEC/ITU와 ANSI X9.45에서는 1996년 6월 확장필드를 추가한 X.509v3을 개발하였다.

X.509v3 인증서 확장필드(X.509v3 Certificate Extensions)는 키와 정책에 대한 정보(Key and Policy Information), 인증서 주체와 발행자에 대한 속성(Certificate Subject and Issuer Attributes), 그리고 인증 경로 제약(Certification Path Constrains)을 포함한다. 그리고, CRL 확장필드(CRL Extensions)는 CRL 번호와 이유 코드(CRL number and reason codes), CRL 분배 지점(CRL distribution points), 그리고 Delta-CRL을 포함한다[1][2][3][4].

2. PGP

PGP(Pretty Good Privacy)는 1991년 6월 Phil Zimmermann에 의해 만들어진 공개키 암호화 프로그램이다. 그 후 1993년 가을에 버전 2.0이 발표된 이래, 현재 버전 6.0이 발표되었다. PGP는 인터넷 전자우편에 신뢰성을 부여하기 위하여 설계되었으며, 메시지를 암호화하고 서명하는데 RSA와 IDEA를 사용한다. PGP 사용자는 통신하는 사람의 공개키를 가지고 있는 키링(keyring)이라는 리스트를 관리한다. 키링은 사용자 자신의 비밀키로 서명되며, 키링에 하나의 키를 추가할 때, 그 키에 서명한다.

사용자들이 키링을 교환할 때, 그들은 신뢰 웹(Web of trust)을 만든다. 많은 방법들 중에, 이것은 PKI에서 가장 단순한 형태이다. 실제로 각 사용자는 자신의 루트 CA가 된다. PGP는 이러한 단순성 때문에 다른 PKI들과 비교해서 상대적으로 널리 사용할 수가 있다. 그러나, 전자상거래와 같은 강한 인증이 요구되는 곳에서는 PGP PKI는 문제점이 있어 사용될 수 없다.

PGP 인증서는 확장될 수 없고, 전자우편 주소, 공개키 값과 신뢰 등급의 속성만을 포함한다. 전자우편 주소가 신원을 확인하는 것에 대한 정확한 수단이 아니기 때문에, PGP는 사람의 신원에 대한 강한 인증을 제공하지 못한다. 그러므로 PGP는 일시적인 전자우편 통신 외에 다른 응용에는 사용되기 어렵다. 또한, PGP는 인증서를 검증하고 취소하는 확실한 방법을 가지고 있지 않다[1][2][16].

3. SDSI

SDSI(Simple Distributed Security Infrastructure)는 안전한 시스템의 구성을 쉽게 하기 위해서, 1996년 Ron Rivest와 Butler Lampson이 버전 1.0을 만들었으며, 1997년에는 버전 2.0이 만들어 졌다. SDSI는 접근 제어 목록(ACL : Access Control List)과 보안 정책을 정의하고 있으며, 신원-기반 인증에서 벗어나 역할과 자격을 기반으로 한 시스템으로 전환을 시도하였다. SDSI 시스템은 신원에 공개키를 포함하는 것이 아니고, 키 자체가 SDSI 개체이다. 특히, SDSI는 당사자(principal)를 호출하고, 그것을 전자서명 검증키로 정의한다. SDSI 당사자는 검증할 수 있는 서명된 문장을 발급함으로써 공개키를 선언할 수 있다[2][7].

3.1 SDSI 이름과 그룹

SDSI는 신원 인증서(Identity Certificates), 그룹-회원 인증서(Group-membership Certificates), 그리고 이름-결합 인증서(Name-binding Certificates)라는 세 가지 형태의 인증서를 제공한다. 그리고 SDSI는 지역 이름 공간을 서로 연결하는 방법을 제공한다. 예를 들어, 사용자 A가 한 당사자를 사용자 B라고 부르고, 사용자 B가 다른 당사자를 사용자 C라고 부른다면, 사용자 A는 두 번째 당사자를 사용자 B의 사용자 C라고 정의할 수 있다.

또한, SDSI는 다중 글로벌 이름 공간을 제공한다. 이것은 분산 루트(Distributed root)라고 하는 당사자에 의해 정의된 이름 공간이다. 이 당사자는 모든 이름 공간 내의 같은 당사자를 가리키는 특정 이름들을 가진다.

SDSI의 당사자는 그룹을 정의할 수 있고, 각 그룹은 이름과 회원을 갖는다. 그 이름은 그룹의 소유자인 당사자에게는 지역적이고, 그룹의 소유자만이 그 정의를 변경할 수 있다.

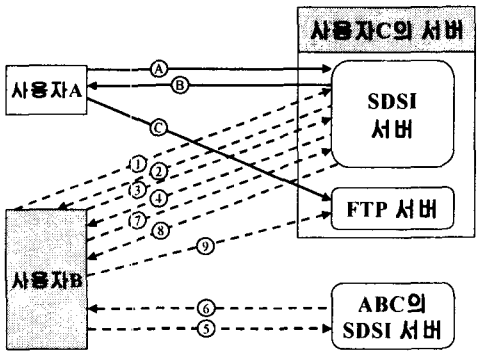
3.2 SDSI 동작

SDSI를 설명하기 위해, SDSI가 어떻게 동작하는지 예를 들어보자. [그림 3-1]은 사용자 C의 그룹과 ABC사의 그룹을 정의하고 있다. [그림 3-2]는 SDSI MemberShip과 Get 프로토콜이 어떻게 FTP 서버에 접근하는데 사용되는지 보여준다. [그림 3-2]는 사용자 C의 친구 그룹에 속한 사용자 A가 어떻게 FTP 서버에 접근할 수 있는지 나타내고, ABC사의 직원 그룹에 속한 사용자 B가 어떠한 과정을 거쳐 FTP 서버에 접근할 수 있는지 나타내고 있다.

사용자C의 그룹	
FTP 사용자	친구
친구 ABC사의 직원	사용자A 사용자D 사용자E

ABC사의 그룹
직원
..... 사용자B1998 사용자C1997 .....

[그림 3-1] 간단한 SDSI 그룹



[그림 3-2] SDSI 프로토콜 예제

Ⓐ 당사자와 그룹 이름 "FTP 사용자"를 포함하는 SDSI Membership.Query 메시지를 전송한다.
Ⓑ 사용자 A에게 "true" 회원 자격 인증서를 전송한다.
Ⓒ 사용자 A는 사용자 C의 FTP 서버에 접근하기 위하여 회원 자격 인증서를 전송한다.

① SDSI 서버에게 Membership.Query를 전송한다.
② 사용자 C의 "ABC사의 직원" 그룹 내에서 사용자 B가 회원이 아님을 나타내는 "fail" 회원 자격 인증서를 전송한다.
③ SDSI Get 프로토콜 Get.Query 메시지를 전송한다.
④ ABC사의 당사자에 대응하는 사용자 C의 지역 이름 ABC를 보여주는 인증서를 전송한다.
⑤ 사용자 B는 ABC사의 SDSI 서버에게 "직원" 그룹에 대한 Membership.Query 메시지를 전송한다.
⑥ 사용자 B에게 "true" 회원자격 인증서를 전송한다.
⑦ 사용자 B는 ABC사의 SDSI 서버로부터 얻은 회원 자격 인증서를 포함해서, 사용자 C의 SDSI 서버에게 "FTP 사용자" Membership.Query 메시지를 전송한다.
⑧ 사용자 B가 "FTP 사용자" 그룹의 회원이라는 것을 검증해서, "true" 회원 자격 인증서를 전송한다.

⑨ 사용자 B는 사용자 C의 FTP 서버에게 "true" 회원 자격 인증서를 전송한다.

4. SPKI

SPKI(Simple Public Key Infrastructure)는 1996년 초 Cybercash사의 Carl Ellison이 중심이 되어 만든 비-X.509 방식으로 개발중인 인증 방법으로, 인증서 내에 최소한의 정보만을 갖는 것을 목표로 하고 있다. 현재 IETF에 인터넷 드레프트로 제출되어 있으며, 계속 수정 보완 중에 있다. SPKI와 SDSI에는 몇 가지 유사한 점이 있다. 특히, SPKI의 요구사항 중 하나는, 가능한 모든 곳에서 SDSI 지역 이름 메커니즘을 지원하는 것이다. SPKI는 SDSI의 당사자(principal) 대신에 키소유자(Keyholder)라는 용어를 사용한다. 이 두 가지는 공개키 값에 자격을 포함하는 메커니즘을 제공한다[2][8][9][15].

4.1 SPKI 인증서

SPKI 인증서는 발행자(Issuer), 주체(Subject), 위임(Delegation), 권한(Authority), 유효성(Validity)으로 5개의 그룹으로 구성되어 있으며, 간단히 (I, S, D, A, V)의 형태로 표현된다. SPKI의 가장 큰 특징은 권한(Authority) 그룹을 이용하여 인증서에 권한을 넣을 수 있다는 것이다. 또한, 다른 사람에게 SPKI 인증서를 발행해 줄 때에는, 발행해 준 인증서에 의해 허가되는 권한을 인증서의 소유자가 다른 사람에게 인증서를 발행함으로써 위임할 수 있다. 그러므로, 위임(Delegation) 그룹을 설정하여 다른 사람에게 권한을 위임할 수 있다. 각 그룹에 대한 인증서의 형식은 [표 3-1]과 같다.

[표 3-1] SPKI 인증서 형식

발행자(Issuer)	인증서를 발행하는 기관
주체(Subject)	인증서에 의해 권한을 부여받은 객체
위임(Delegation)	권한을 위임할 수 있는 가에 대한 플래그
권한(Authority)	인증서의 소유자가 행할 수 있는 권한
유효성(Validity)	유효 기간

4.2 인증 방법

SPKI에서는 인증서 내에 권한을 첨가할 수 있는 방법을 사용하고 있다. 일반적으로 인증서의 유효성을 검증하여 신원을 확인하고 이를 이용하여 권한을 얻어내 어떤 요청을 허가해 주는 것과는 달리, SPKI는 인증서 자체에 권한을 넣을 수 있어 인증서 자체에 대한 유효성만 검증되면 권한에 해당하는 요청을 허가해 줄 수 있다. SPKI에서 일반적으로 사용될 수 있는 권한들은 [표 3-2]와 같다.

[표 3-2] SPKI 권한

권 한	예 제
Member-of-issuer	Moi
Name	Name fred
Member	Member faculty
FTP	FTP cybercash.com cme
HTTP	HTTP http://acme.com/company-private/personnel/
TELNET	TELNET erols.com spinne

Ⅳ. PKI 시스템 비교

현재 공개키 기반구조에는 뚜렷한 구조를 가지고 있는 X.509와 X.509 기반의 PEM이 있고, 특정 구조가 없는 비-X.509 기반의 PGP, SDSI, SPKI가 있다. PEM은 X.509v1을 이용하여 인증서 내에 여러 가지 정보를 포함하여 정보보호 서비스를 제공하지만, 많은 문제점을 내포하고 있다. 또한, X.509v3의 경우도 확장필드(extensions)를 이용하여 이 문제점을 해결하려고 시도하였지만 구현이 쉽지 않다. PKIX(X.509v3을 이용한 공개키 기반구조) 작업이 계속 되고 있으나, X.509에 기반한 PKI의 구현에 문제점이 많아, 작업이 매우 느려지고 있다.

이러한 X.509 기반 시스템의 구현상 어려움 때문에, 일부에서는 비-X.509 시스템을 만들어 사용하려는 시도를 하고 있다. 가장 대표적인 것은 간단한 신뢰-웹 상의 인증서에 단순히 공개키, 전자우편 주소, 그리고 신뢰 등급만을 가지는 PGP, 인증서의 형식을 대폭으로 축소하여 안전한 시스템을 목표로 하는 SDSI와 인증서 자체에 권한을 부여하는 방식으로 5-TUPLE이라는 인증서 형식을 사용하는 SPKI가 있다. 그리고, SDSI 인증서와 SPKI 인증서는 서로 호환이 가능하다. 하지만, PGP는 강한 인증에 사용될 수 없다는 단점을 가지고 있으며, 현재 SDSI나 SPKI도 인터넷 드레프트 상태에서 크게 발전되지 않고 있다.

1. 인증 구성 객체와 구조

X.509 기반의 공개키 기반구조를 구성하려면 기본적으로 인증기관, 조직 등록기관, 그리고 인증서 사용자를 필요로 한다. 인증기관은 여러 등급으로 나누어지고 서로 하는 역할도 다르지만, 비-X.509 기반의 공개키 기반구조를 구성할 때에는, 인증기관을 사용하지 않는다. [표 4-1]은 각 PKI 시스템이 기본적으로 갖는 구성 객체를 분류한 것이다.

[표 4-1] 인증 구성 객체에 따른 분류

객 체	의 미	X.509	PEM	PGP	SDSI	SPKI
인증기관	인증서를 발급한 기관	○	○		○	○
등록기관	인증서의 발급을 등록하는 기관	○	○			
인증서 소유자	인증기관에 의해 인증서를 받은 자	○	○	○	○	○
클라이언트	인증서를 사용하는 자	○	○	○	○	○
저 장 소	저장 및 검색하는 장소	○	○			

여기서 또, 인증기관의 구성은 PAA, PCA, 그리고 CA로 구분된다. 하지만, 각 공개키 기반구조 시스템들은 자신의 시스템에 맞는 구조를 만들어 사용하고 있다. 계층구조의 PKI 시스템은 최상위 계층에 PAA를 두고, 제2계층에 PCA, 제3계층에는 CA 또는 RA를 두며, CA는 하위에 다른 CA들로 구성될 수 있다. 국가별 인증기관의 계층은 [표 4-2]와 같다.

[표 4-2] 각국의 인증기관 구조에 따른 분류

인 증 기 관		미국	캐나다	호주	유럽
		NIST	CSE	PKAF	ICE-TEL
PAA	정책 승인 기관	PAA	PAA	PKAF	ICE-TEL CA
PCA	정책 인증 기관	PCA	PCA	ICA	PCA
CA	인증 기관	CA	CA	OCA	CA
RA	등록 기관	ORA	ORA	ORA	RA

2. 인증서 검증 및 취소

인증서 검증은 인증서의 데이터가 정당한지를 확인하는 과정이다. 각 공개키 기반구조 시스템에서 인증서를 검증하는 방법에는 크게 온라인 검증과 오프라인 검증으로 구분할 수 있다. 이들 방법은 서로 장·단점을 가지고 있지만, 온라인 방법을 기본으로 해서, 오프라인 방법을 최소화해야 한다. [표 4-3]은 인증서 검증 및 취소에 따른 분류를 나타내고 있다. [표 4-4]는 각국의 인증서 취소 정책에 따른 분류이다.

[표 4-3] 인증서 검증 및 취소에 따른 분류

방 법	의 미	X.509	PEM	PGP	SDSI	SPKI
온라인	인증서를 사용할 때마다 확인	○				○
오프라인	인증서를 사용할 때 CRL을 이용	○	○	○	○	○
CRL	인증서 취소 목록	○	○			○
Delta-CRL		○				○

[표 4-4] 각국의 인증서 취소 정책에 따른 분류

구 분	미국	캐나다	호주	유럽
CRL 형식	X.509v2	X.509v2	X.509v2	X.509v2
CRL 생성	온라인 방법 : 취소 이유 발생시			
	오프라인 방법 : 주기적인 CRL 발급			
CRL 획득	디렉토리 서비스			
	데이터베이스			
확장필드	사용	사용	CRL 발급 번호	CRL 발급 번호
			취소 이유 코드	취소 이유 코드

3. 알고리즘

공개키 기반구조는 전자 서명 알고리즘과 메시지 인증 알고리즘을 사용한다. X.509 인증서는 인증서를 서명하는데 이용되는 알고리즘과 주체의 공개키 에 대한 알고리즘을 기술한다. 여기에서 두 알고리즘은 다를 수도 있다. 인증기관과 최종객체는 RSA, DSA, ECDSA 중 하나를 이용할 수 있어야 한다. 즉, 클라이언트는 3개의 알고리즘 모두에 대해 서명을 검증할 수 있어야 한다. 메시지 인증 알고리즘에는 데이터에 대한 DES MAC을 계산함으로써 무결성을 제공한다. 공개키 기반구조에 사용되는 알고리즘을 분류하면 [표 4-5]와 같다.

[표 4-5] 사용 알고리즘에 따른 분류

기반구조 / 알고리즘		X.509	PEM	PGP	SDSI	SPKI
전자서명	RSA	○	○	○	○	○
	DSA	○				
	ECDSA	○				
	MD2		○			
	MD5		○	○	○	○
	SHA1				○	○
메시지인증	RSA	○	○	○	○	○
	DES	○	○			
	DES MAC	○				
	IDEA			○		

V. 결론

현재 널리 사용되고 있는 전자상거래의 안전성과 신뢰성을 확보하고, 전자서명의 생성과 인증 등에 필요한 절차를 정하고, 네트워크를 통하여 공개키와 인증서를 체계적으로 관리하기 위해서는 공개키 기반구조 기술이 필요하다. 이러한 공개키 기반구조 기술을 통해 공개키 암호시스템을 사용하여 비밀키의 기밀성과 공개키의 무결성 서비스를 제공할 수 있다.

본 논문에서는 현재 널리 사용되고 있는 전자상거래를 위해서, 필수적인 공개키 기반구조에 대하여 분석하였다. 이러한 공개키 기반구조가 활성화되기 위해서는, 기본이 되는 공개키 암호화 기술, 전자 서명 기술 등 많은 기술이 선행적으로 이루어져야 하고, 이러한 기술들을 바탕으로 공개키 기반구조의 구성 객체에 대한 정보보호를 확립해야 한다. 그러나, 이렇게 보호된 구성 객체들을 어떻게 구성해야 하는지가 아직 해결해야할 문제이다.

먼저, 안전한 전자상거래를 위해 필요한 선행 조건들을 몇 가지 들 수 있다. 첫 째, 범국가적인 인증정책의 마련이 시급하다. 둘 째, 이 인증정책을 승인하고 관리하는 기구의 설립이다. 셋 째, 이러한 것을 해결할 수 있는 기술을 산·학·연이 공동으로 표준화 작업을 해야 하며, 마지막으로는 전자상거래와 관련된 법률의 제정과 정비이다.

현재까지 제안된 비-X.509 기반의 공개키 기반구조들은 X.509 기반의 공개키 기반구조가 가지고 있는 문제점을 해결하고자 설계되었지만, X.509 기반의 공개키 기반구조의 확장필드를 잘 운영하면 보다 나은 보안구조를 설계할 수 있다.

본 논문에서는 공개키 기반구조에 대해 분석하였다. 여기서 분석된 자료들은 PKI 설계자들에게 기본적인 방향을 제시할 수 있고, PKI 개발자들의 요구에 적합한 PKI 시스템을 선택할 수 있도록 도와줄 것이다.

[참고문헌]

[1] W. Ford & M. S.Baum, "Secure Electronic Commerce", Prentice Hall PTR, 1997

[2] Marc Branchaud, "A Survey of Public Key Infrastructures", McGill University, 1997

[3] R. Housley, W. Ford, W. Polk, D. Solo, X.509 Certificate and CRL Profile, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-07.txt, 1998. 3

[4] C.Adams, S. Farrell, Certificate Management Protocols, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-08.txt, 1998. 5

[5] GOC Public Key Infrastructure, http://www.cse.dnd.ca/cse/english/gov.htm

[6] Standards Australia, Strategies for the implementation of a Public Key

Authentication Framework(PKAF) in Australia, SAA MP75-1996

[7] Morcos, Alexander, A Java Implementation of Simple Distributed Security Infrastructure, 1998, 5,
http://theory.lcs.mit.edu/~cis/theses/morcos-masters.ps

[8] Simple Public Key Infrastructure : Theory(draft-ietf-spki-cert-theory-03.txt), 1998. 10. 18.

[9] Simple Public Key Infrastructure : Structure(draft-ietf-spki-cert-structure-05.txt), 1998. 3. 13.

[10] 임신영, 유창열, 송유진, 함상호, 박상봉, "전자 상거래를 위한 공개키 기반 인증 기술", 통신정보보호학회지, 제7권, 제3호, 1997. 9.

[11] 김지연, 박성준, "공개키 기반구조에 관한 고찰", 통신정보보호학회지, 제7권, 제2호, 1997. 6.

[12] 한국정보보호센터, "국외 공개키 기반구조 추진체계 분석", 1998. 7.

[13] 한국정보보호센터, "PKI 구성 객체의 상호연동성을 위한 명세서 분석", 1998. 7.

[14] 한국정보보호센터, "공개키 기반구축에 관한 연구", 1997. 12.

[15] 한국과학재단, "인터넷 상점에 대한 신용 인증 기술", 1998.

[16] 최용락, 소우영, 이재광, 이임영, "통신망 정보 보호", 도서출판 그린, 1997.