기술문서	‘08. 10. 30. 작성

P K I

(Public Key Infrastructure)

작성자 : 영남대학교 *@Xpert* 강정희
o1116@ynu.ac.kr

- Contents -

0. 개 요

컴퓨터 네트워크를 통해 안전한 비즈니스와 기밀성이 보장되는 통신을 하기 위한 방법 중의 하나로 공개키 기반 구조를 사용한다. 이 문서는 공개키 기반 구조(PKI)를 이해하기 위한 것으로서 PKI에 논하기에 앞서 '1. 암호'에서는 암호에 대한 전반적인 개념과 종류에 대해 소개한다. '2.PKI' 에서는 PKI의 개념과 전문용어 소개, 구성 등을 소개 한다.

1. 암 호

통신문의 내용을 제3자가 판독할 수 없는 글자·숫자·부호 등으로 변경시킨 것으로 로마시대 이후부터 널리 고안되어 사용되고 있다. 14세기 이탈리아에서 근대적인 암호가 개발되었으며 무선통신의 발달, 세계대전 등으로 암호화, 암호해석 기술이 획기적으로 발달하였다.

가. 암호(暗號)의 정의

현대 암호학은 이를 훨씬 뛰어넘어 전자 서명, 저작권 관리, 신원 확인 등의 기능까지도 수행하고 있고, 암호학을 이용한 공개키 기반 구조는 인터넷 시대의 안전성과 신뢰성 확보를 위한 필수 요소로 꼽히고 있다. 인터넷 환경에서의 암호는 비밀 인증 데이터의 한 형식으로 어떠한 자원에 대한 접근을 제어하는 데에 사용되는 것을 의미한다.

나. 암호의 문제점

인터넷을 이용한 전자 문서의 전달 과정에서 발생할 수 있는 문제점은 크게 4가지로 구분되며, 이런 기본적인 4가지 문제를 해결하기 위한 방법을 연구하는 것이 암호학(Cryptography)의 한 분야이다.

1) 기밀성(Confidentiality)

부적절한 노출 방지. 전달된 데이터를 제 3자가 읽지 못하도록 비밀성을 유지하는 기능

o 문제점

송신자와 수신자가 주고받는 전자 문서의 내용은 송신자와 수신자만이 알아야 하지만, 인터넷과 같이 전자 문서가 전달되는 통신망이 공개되어 있는 경우에 전자 문서의 내용이 공격자에게 노출될 수 있다.

o 해결 방안

통신망을 통해 전달되는 전자 문서의 형태를 변형하여 공격자가 이해할 수 없도록 한다. 일반적으로 이렇게 전자 문서를 변형하는 과정을 암호화라고 한다.

2) 인증(Authentication)

허가받은 사용자가 아니면 내용에 접근할 수 없어야 한다.

o 문제점

- 사용자 인증 : 송신자와 수신자 사이에는 인터넷이 존재하므로 수신자는 자신에게 접속하는 송신자가 적정한 송신자인가를 확인할 수 없다.
- 전자 문서 인증 : 수신자가 전자 문서를 받았을 때 적정한 사용자가 보낸 전자 문서가 위·변조 없이 도착했는가를 확인할 수 없다.

o 해결 방안

- 사용자 인증 : 상대방이 원하는 경우에 자신임을 증명할 수 있는 정보를 제공할 수 있어야 한다.
- 전자 문서 인증 : 전자 문서와 송신자 간의 연관성 있는 증명 정보를 생성하여 상대방에게 전자 문서와 같이 전달하고 수신자는 증명 정보를 검증하여 문서의 진위성을 확인한다.

3) 무결성(Integrity)

부적절한 변경 방지. 권한이 없는 방식으로 변경되거나 파괴되지 않는 데이터의 특성을 말하며 데이터를 보호하여 언제나 정상적인 데이터를 유지한다.

o 문제점

인터넷을 통해 전달되는 전자 문서가 중간에 공격자에 의해 또는 통신 과정상의 오류발생으로 위조 또는 변조되었는가를 확인할 수 없다.

o 해결 방안

전자 문서를 수신자에게 전달할 때 전자 문서에 대한 고유한 증명 정보를 생성하여 전자 문서와 같이 보내고, 수신자는 수신한 전자 문서에 대해 송신자가 증명 정보를 생성한 동일한 방법으로 증명 정보를 생성하여 수신한 증명 정보와 동일한지 확인한다.

4) 부인 방지(Non-Repudiation)

메시지를 전달하거나 전달받은 사람이 메시지를 전달하거나 전달받았다는 사실을 부인 할 수 없어야 함.

o 문제점

전자 문서는 무제한의 복제 가능성을 가지고 있다. 그러므로 전자 문서를 생성하거나 송·수신한 사실을 전자 문서의 생성자나 송수신자가 부인하는 경우에 이를 증명할 수 있는 방법이 없다.

o 해결 방안

전자 문서에 전자 서명을 하거나 전자 문서를 송·수신하는 행위에 대해 전자 서명을 하여 사후에 부인을 방지하지 못하도록 한다.

다. 암호의 종류

암호학을 이용하여 보호해야 할 메시지를 평문(plaintext)이라고 하며, 평문을 암호학적 방법으로 변환한 것을 암호문(ciphertext)이라고 한다. 이때 평문을 암호문으로 변환하는 과정을 암호화(encryption)라고 하며, 암호문을 다시 평문으로 변환하는 과정을 복호화(decryption) 라고 한다. 평문과 암호문의 전환과정에서 입력되는 정보를 키(Key)라고 한다. 키의 특성에 따라 두 가지로 구분된다.

1) 대칭키 (Symmetric Key)

비밀키 암호 방식이라고도 하며, 송신자가 소유한 비밀키로 평문을 암호화 시키면 그 암호문을 수신한 사람은 암호화 시킬 때 사용한 동일한 키를 사용하여 복호화 한 뒤 원래의 평문의 내용을 볼 수 있다. 동일한 키를 사용하기 때문에 암호화 복호화 속도 면에서 비대칭키 알고리즘에 비해 빠르다는 장점이 있지만 키 관리 문제에 치명적인 허점을 드러내고 있는데 그것이 바로 키 관리 문제이다. 대표적인 대칭키 알고리즘으로는 DES , 3DES , AES , SEED등이 있다.

2) 비대칭키(Asymmetric key)

공개키 암호 방식이라고도 하며, 대칭키의 단점인 키 관리의 문제점을 보완하기 위해 나온 방법으로 메시지를 송신하는 자는 수신하는 사람의 공개키로 암호화하여 전송하고 수신하는 자는 생성한 키 쌍 중의 개인키로 복호화하여 평문을 획득한다. 키 관리가 편리하다는 장점이 있으나 알고리즘의 복잡한 수학적인 성질에 기초하다 보니, 그것을 연산하려면 속도가 좀 느리다. 대표적인 알고리즘으로는 RSA, Elliptic Curve ElGamal, DH(Diffie-Hellman), ECC 등이 있다.

종 류 / 속 성	비 밀 키	공 개 / 개 인 키
사 용 기 간	천년정도	50sswjd도
주로 사용되는 이유	일반데이터 암호화	키교환, 전자서명
현재표준	DES, 3중 DES, AES	RSA, Diffie-Hellman, DSA
암호화/복호화 표준	빠르다	느리다
키	최소 두 사람 사이에서 교환	개인키: 한 사람에 의해서만 관리 공개키: 어디서든지 배포 가능
키 교환	교환하는 것은 어렵고, 위험	개인키: 비밀로 간직 공개키: 전달 용이
키 길이	56비트, 128비트(권장)	1024비트 사용(RSA), 어떤 경우에는 2048비트(단, ECC는 72비트-휴대단말기에서 이용)
기밀성, 인증, 메시지 무결성	가 능	가 능
부인 방지	불가능(제 3자 필요)	가능(전자 서명 사용)
공 격	있 음	있 음

표 2 . 비밀키와 공개/개인키의 특징

PKI를 알아보기 전에 기본 지식으로 암호의 종류를 분류하였기 때문에 자세한 언급은 하지 않도록 한다.

2. PKI(Public Key Infrastructure)

공개된 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 등장한 것이 공개키 기반구조(PKI)이다. 공개키 기반구조에서는 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서(certificate)를 공개한다. 인증서는 신뢰할 수 있는 제 3자(인증기관)의 서명문이므로 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다.

가. 용어정리

1) 인증기관(CA: Certification Authority)

인증 정책에 따라 인증서를 생성하거나 취소하는 객체(entity)로 모든 인증기관들은 자신의 키 쌍을 생성하고 선택적으로 사용자의 키를 생성할 수 있다.

2) 인증서(certificate)

인증 기관의 비밀키로 암호화되어 위조할 수 없는 사용자의 유일한 이름, 사용자의 공개키 및 기타 정보로 이루어진 문서로 인증서를 발행한 CA의 인증 정책도 포함한다.

3) 인증정책(certification policy)

인증정책은 CA가 작동하는 메커니즘과 사용되는 암호 알고리즘과 서명 알고리즘, 최소 키 크기, 인증서 유효의 최대 길이, 인증서 취소 목록 갱신의 최대 기간, 인증서를 발행하기 위해 사용자의 신분을 확인하는 메커니즘 등을 기술한다. 정책은 객체 식별자(OID: Object Identifier)로 명명되고 정책의 OID는 그 정책 하에 발행된 모든 인증서 내(extension 영역)에 포함된다.

4) 보안 정책(security policy)

보안 서비스 및 기능의 제공을 관리하는 보안 기관에 의한 규칙들이다.

5) 도메인(domain)

공통적인 보안 정책을 구현하거나 밀접하게 관련 있는 명명공간(namespace) 내에 사용자들에 대해 인증서를 발행해주는 CA들이 논리적으로 그룹화 되어있는 것을 도메인이라 한다.

6) 상호인증서(cross-certificate)

한 CA가 다른 CA를 신뢰하여 그 CA에 인증서를 발행할 때 그 인증서를 상호인증서라 한다. 한 CA를 신뢰하는 모든 객체는 그 CA가 상호 인증한 CA에 의해서 발행된 모든 인증서를 신뢰한다.

7) 인증 경로(certification path)

경로상의 최종 객체에 대한 공개키를 얻기 위한 인증서들의 정렬된 순서로 A→B는 A로부터 B로의 인증 경로를 나타낸다. A→B는 A의 인증서로 시작되어 B의 인증서로 끝나는 고리의 형태인 CAA<<A>>…CAB<<B>>로 구성된다.

8) 디렉토리(directory)

객체에 대한 정보 저장소로 사용자들로 하여금 그 정보에 접근할 수 있는 서비스를 제공한다.

9) 신뢰(trust)

일반적으로 한 실체는 다른 실체가 자신의 기대한 바와 같이 행동을 하리라고 가정할 수 있을 때 실체는 다른 실체를 신뢰한다고 말할 수 있다. 이러한 신뢰는 일부 특정 기능에만 적용될 수 있다. 인증 프레임워크에서 이 신뢰의 주요 역할은 인증하려는 실체와 인증 기관간의 관계를 기술하는 것으로 인증하려는 실체는 인증기관이 유효하고 신뢰할만한 인증서를 생성한다고 확신할 수 있어야 한다.

나. 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다. 다시 말해 이것은 사용자의 공개키가 실제로 사용자의 것임을 증명한다. PKI에서 인증서의 발행대상은 인증기관 과 사용자, 서버등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다. 인증서는 여러 가지 형태가 있을 수 있지만 현재 가장 많이 사용되는 것은 ITU-T에서 정한 X.509이며, 버전 3이 가장 많이 사용되고 있다.

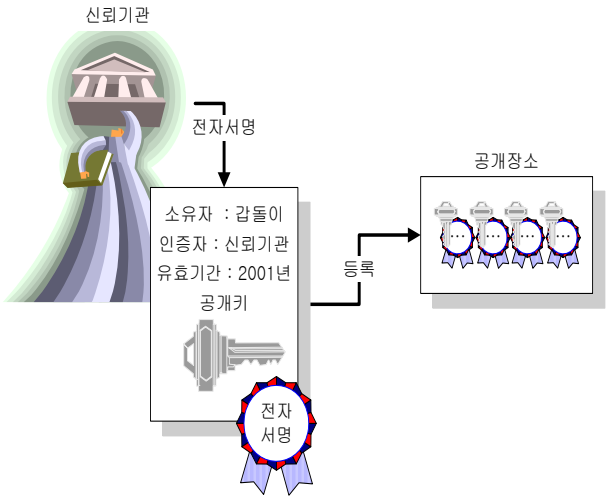

그림1. 인증서의 생성

인증서는 신뢰 기관이 발급하는 것이고 사용자의 정보를 포함하고 있기 때문에 나름대로의 생명 주기(Life Cycle)가 있다. 먼저 사용자는 인증서를 신뢰 기관으로부터 발급받는다. 사용자는 발급된 인증서를 사용하다가 인증서의 효력을 정지시킬 수 있고, 자신이 사용하는 비밀키와 공개키에 문제가 있다고 판단되는 경우에는 이를 변경하여 재발급 받을 수도 있다. 또한, 인증서가 필요 없는 경우에는 인증서를 폐지할 수도 있다. 이런 일련의 과정을 인증서의 생명 주기라고 한다.

다. 상호인증서쌍(cross-certification pair)

한 도메인이나 서로 다른 도메인의 인증기관들 사이에 발행하는 인증서로 두 가지 형태가 있다. 이것은 쌍을 이뤄 각 인증기관(X)의 엔트리로 디렉토리에서 관리된다.

1) 순방(forward) 인증서

인증기관 X에 대해 다른 인증기관에서 생성한 인증서

2) 역방(reverse) 인증서

인증기관 X가 다른 인증기관에게 생성한 인증서

상호 인증서를 사용함으로써 같은 도메인 내에서는 인증 경로를 단축할 수 있고 서로 다른 도메인내의 사용자들에게는 그들 간의 안전한 통신 수단을 제공할 수 있다. 디렉토리에서 관리된다.

라. PKI 구성 요소

PKI를 구성하는 최소 객체들은 등록기관(RA:Registration Authority), 인증기관, 디렉토리, 사용자이다

1) 인증기관

PKI를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 여러 명칭으로 불리운다. 아래 세 기관 모두를 통틀어 인증기관이라 한다.

- o 정책승인기관(PAA:Policy Approving Authority)

  I구축의 루트 CA로의 역할

- o 정책인증기관(PCA:Policy Certification Authority)

  PAA 아래 계층으로 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서취소목록 등을 관리한다.

o 인증기관(CA: Certification Authority)

인증서를 발행/취소, 공개키 전달, 상호 인증서 발행, 데이터베이스 관리

2) 등록기관(RA)

인증기관과 물리적으로 멀리 떨어져 있는 사용자들을 위해 인증기관과 인증서 요청 객체 사이에 등록 기관을 둠으로써, 사용자들의 인증서 신청 시 인증기관 대신 그들의 신분과 소속을 확인하는 기능을 수행한다. 인증서 요청에 서명을 한 후 인증기관에게 제출하거나 사용자에게 직접 전달한다.

3) 디렉토리

인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서취소목록등을 저장 및 검색하는 장소로 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에 일정 기간 동안 서명 검증의 응용을 위해 디렉토리에 저장된다.

4) 사용자

사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

마. PKI 구성

PKI에서 신뢰는 인증 경로를 통해 전달된다. 인증서 검증 단계에서 다수의 CA가 엮이므로, CA 간 신뢰 모델이 전체 PKI 동작에 중요한 역할을 함.

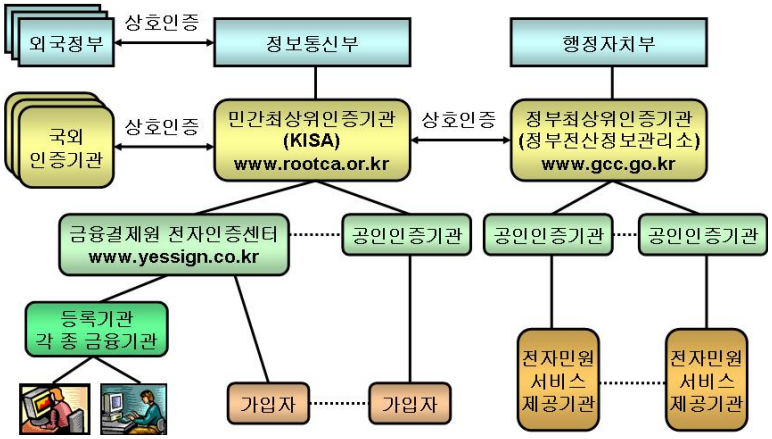

그림 2 . 국내의 PKI 구성 구조도

1) 계층구조 구성:

모든 인증기관이 단일 계층구조를 형성. 부모 인증기관이 자식 인증기관의 인증서를 발급하고 단말 인증기관이 일반 가입자의 인증서를 발급. 루트 인증기관은 자신을 인증할 기관이 없으므로 자체 서명 인증서를 사용한다.

장 점	단 점
원하는 인증서의 획득이 용이하다. 인증경로에 대한 검증이 용이하다. 계층적인 조직에 적합하다	현실적으로 전 세계적인 구성이 불가능하다. 루트 인증기관의 비밀키 안정성이 모든 인증서의 안전성과 관계가 있다.

표 3 . 계층구조 구성의 장·단점

2) 네트워크 구성

네트워크 구조는 일반적인 네트워크 환경에서 근접한 인증기관에 대해 상호인증을 할 수 있는 구조이다. 인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구조로서, 인증기관들이 상호 인증하며 인증서를 발급한다. 사용자는 인증서를 발행한 인증기관의 공개키만을 알고 있다. 이 구조에서 인증서를 얻기 위한 인증 경로는 일반적으로 사용되는 라우팅 방법과 동일하게 최단 거리 알고리즘이 적용되며, 경로는 하나 이상이 될 수 있다.

장 점	단 점
인증기관 간의 상호인증 상업적 상호신뢰 관계 유리 융통성 있는 정택과 처리부하의 경감 CA의 비밀키 손상에 대한 복구 용이	원하는 인증서를 찾기위한 인증경로체계와 관리의 복잡성 단일 인증경로 불가능

표 4 . 네트워크 구성의 장·단점

3) 혼합 구성

계층 구조와 네트워크 구조를 혼합한 구조이다. 구조적인 특징으로, 커다란 조직에 대해서 각각 루트 인증기관이 존재하고, 각 루트 인증기관은 자신의 하위 인증기관에 대해서 인증하며, 동일 계층에 존재하는 기관은 다른 루트 인증기관과 상호 인증을 한다. 루트 인증기관의 하위 인증기관은 동일 계층의 인증기관간의 상호 인증이 가능하여 자신의 하위 및 상위 인증기관과의 인증이 가능하다. 따라서 계층 구조처럼 하나의 인증서를 갖고 있으며, 다른 인증기관에 대한 인증서는 디렉토리에 저장된다. 네트워크와 계층적인 인증 경로의 좋은 요소를 결합하여 구성되면 위 두 가지의 인증 경로보다 더 유용하다.

4) 기타 구성

푸시(push), 풀(pull), 독점, 소수 독점 모델 등. 인증서 검증 단계에서 다수의 CA가 엮이므로, CA 간 신뢰 모델이 전체 PKI 동작에 중요한 역할을 함.

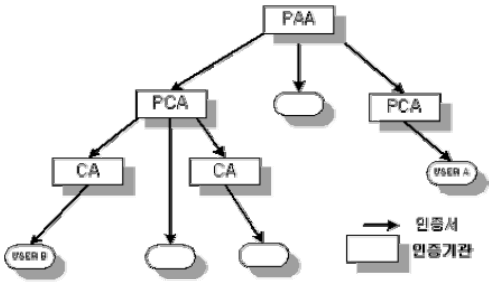

그림 3 . 계층구조 구성

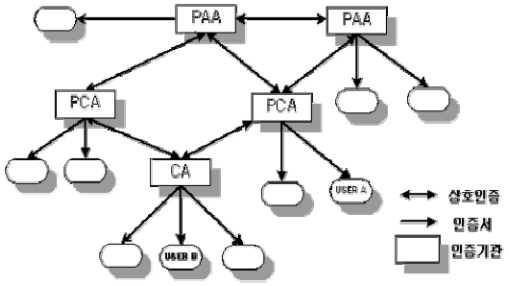

그림 4 . 네트워크구조 구성

바. 인증서 폐기 목록(Certificate Revocation List, CRL)

말소 기한이 되기 전에 취소된 인증서(certificate)들의 목록으로서 폐기된 인증서들을 이용자들이 확인할 수 있도록 그 목록을 배포, 공표하기 위한 메커니즘을 포함한다. CRL은 인증기관(CA)에서 관리하는데, 인증기관은 발급한 인증서의 변경 및 취소 요청이 있을 경우에 해당 인증서를 CRL에 등록한다. 인증서 폐기 목록(CRL)에는 취소된 인증서들의 일련번호가 들어 있다. 사용자는 인증서의 유효성을 검증 시, 인증서의 일련번호가 CRL에 등록되어 있으면 이를 받은 당사자는 목록을 참조하여 그 인증서는 효력이 없는 것으로 판단하고, 취소된 인증서를 사용하지 않도록 해야 한다. 인증서가 취소되고 CRL이 만들어져야 하는 데는 몇 가지 이유가 있다. 예를 들어 인증서가 누설(compromise)된 것이거나 인증서의 소지자가 더 이상 자신이 소유하던 키를 사용할 수 없는 경우가 있을 수 있다.

3. 결 론

전 세계적으로 인터넷을 사용하는 현재. 인터넷 없이는 살 수 없는 현재. 인터넷 비즈니스가 보편화되어 있는 현재지만, 보안이라는 필수사항을 등한시하는 보안 불감증을 먼저 꺼내본다.

인터넷의 급속한 확산과 전세계 통신서비스의 확장으로 세계는 정보의 공유와 이용을 통해 다양한 삶의 변화를 가져오고 있다.

전 세계가 정보화의 물결 속에서 보다 신속하고 안전한 정보의 교류를 위한 기술의 개발 및 연구는 시간의 변화와 더불어 신속하게 변화되어지고 있다. 정보의 중요성과 효용가치의 증대는 다양한 분야에서의 기술발전을 함께 필요로 하게 되었고 특히 정보 보호의 필요성은 그 핵심 기술로 자리 잡게 되었다.

특히 공개키 기반 기술은 개방 네크워크상에서 안전하고 건전한 서비스가 이루어질 수 있도록 통신 정보의 비밀성, 인증성, 무결성, 부인방지 등 기본적인 보안 서비스를 가장 효과적으로 제공하는 기술이다. 따라서 개방적이고, 세계화한 암호기술 사용 환경이 필요하고 이를 효율적으로 적용 및 활용할 수 있는 것이 공개키 기반구조인 것이다.

PKI 기술은 인터넷 환경을 구축하는 네트워크 기술처럼 정보보호 서비스를 위한 기반 기술 요소로서 PKI 구축은 곧 인프라 개념으로 볼 수 있다. 따라서 몇몇 업체나 기관에 의해 구축되어지는 것이 아닌 정보, 정보보호 개발 업체, 서비스 업체 및 연구기관 등 다양한 분야의 기술과 정책이 어우러져야 비로소 그 효과를 얻을 수 있는 기술이라고 할 수 있다.

4. 참고문헌 및 참고 사이트

[1] H.X Mel & Doris Baker 공저 정재원 류대걸 강한 공역 "보안과 암호화 모든 것"
[2] 칼리슬 아담스, 스티브 로이드 공저 장기식 역 "보안을 위한 효율적인 방법 PKI"
[3] http://tadoli.springnote.com/pages/1064412 tadoli님의 노트
[4] 특허청, 한국발명진흥회 1.2-4 공개키 기반 구조(PKI: Public Key Cryptography)