**PKI (Public key Infrastructure)**

**Reference:** [**https://www.tutorialspoint.com/cryptography/public\_key\_infrastructure.htm**](https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Key management에 대한 주요 사항**   암호화 키는 특별한 데이터의 조각이다. Key management는 **암호화 키에 대한 보안 관리**이다.  Key management는 key의 전체 생명주기를 다룬다. Key의 생명주기는 오른쪽 그림과 같다.  **[public key 보안에 대한 key management의 요구사항]**   |  |  | | --- | --- | | Private key의 기밀성 | 전체 key 생명주기에서 secret key는 소유자와 사용이 허가된 자를 제외하고 secret(접근이 불가능)이어야 한다. | | Public key의 보증 | Public key는 public한 데이터이다. 이때 기본적으로 public key가 정확하다는 보장이 없으므로 public key management는 public key의 보증에 초점이 맞춰져야 한다.   * **PKI(public key infrastructure)를 통해 달성**될 수 있다. | |

|  |
| --- |
| 1. **Public Key Infrastructure (PKI)**   **Public Key Infrastructure (PKI):** **public key들과 그것들의 distribution을 identify하고, public key의 정확성을 보증**한다. PKI는 다음과 같이 구성된다.   * Public Key Certificate = Digital Certificate (디지털 증명서) **(3)** * Certification Authority **(4)** * Registration Authority **(5)** * Certificate Management System **(6)** * Private Key Tokens **(7)** |

|  |
| --- |
| 1. **Digital Certificate (디지털 증명서)**   디지털 증명서는 사람뿐만 아니라 소프트웨어 패키지 등 identity를 필요로 하는 다른 것에 대해서도 발급된다.   * Public key와 certification validation에 대한 표준 인증 포맷을 정의하는 ITU standard X.509에 기초한다. * **Certification Authority (CA):** User client와 관련된 public key는 관련된 정보(client info, expiration date 등)와 함께 CA에 의해 디지털 증명서에 저장된다.   + Public key에 대한 보증 및 client에 대한 보증된 정보가 필요하면 CA의 public key를 이용하여 signature validation을 수행한다. |

|  |
| --- |
| 1. **Digital Certificate (디지털 증명서)**   **[디지털 증명서를 얻는 방법]**  CA는 다음 작업을 수행한다.   1. client의 application을 받아서 public key를 인증한다. 2. client의 identity를 verify한다. 3. client에게 디지털 증명서를 발급한다. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Certifying Authority (CA)**   CA는 client에게 디지털 증명서를 발급하고 다른 유저들이 그 증명서를 verify할 수 있도록 돕는다. 또한 client의 identity를 정확히 identify하고, 증명서의 정보가 정확하며 디지털 서명이 되어 있을 것을 보장할 책임을 진다.  **[CA의 key functions]**   |  |  | | --- | --- | | Generating key pairs | CA는 독립적으로/다른 클라이언트와 함께 key pair를 생성한다. | | Issuing digital certificates | CA는 클라이언트가 identity를 확인하기 위한 증명을 제공한 후 디지털 증명서를 발급해야 한다. | | Publishing certificates | CA는 사용자들이 찾을 수 있도록 디지털 증명서를 발표해야 한다. | | Verifying certificates | CA는 클라이언트들이 디지털 증명서를 verify할 수 있도록 돕기 위해서 public key를 사용할 수 있게 해야 한다. | | Revocation of certificates | CA는 client의 신뢰 상실 등의 이유로 경우에 따라 디지털 증명서를 폐기해야 한다. |   **[Class of Certificates]**  디지털 증명서에는 다음 4가지의 종류가 있다.   |  |  | | --- | --- | | Class 1 | 이메일 주소를 통해 증명서를 쉽게 얻을 수 있다. | | Class 2 | 증명서를 발급하는 데 추가적인 개인정보가 필요하다. | | Class 3 | 증명서는 요청자의 identity가 확인된 후에만 발급될 수 있다. | | Class 4 | 증명서는 높은 신뢰가 필요한 정부 또는 금융 기관 등에서 사용한다. | |

|  |
| --- |
| 1. **Registration Authority (RA)**   CA는 identity를 증명하려는 사람 또는 회사의 necessary check를 수행하기 위하여 third-party Registration Authority (RA)를 사용할 수 있다.   * RA는 CA의 client처럼 보이지만 실제로는 발급된 증명서를 sign하지 않는다. |

|  |
| --- |
| 1. **Certificate Management System (CMS)**   **CMS:** 디지털 증명서가 발표되고, 효력이 일시 또는 영구적으로 정지되고, renewal되고, 폐기되는 과정에서의 관리 시스템   * 특정 시점에 상태를 증명하는 데 필요하기 때문에 보통은 증명서를 삭제하지 않는다. * 연관된 RA와 함께 있는 CA는 responsibility와 liability를 tracking하기 위하여 CMS를 실행시킨다. |

|  |
| --- |
| 1. **Private Key Tokens**   Client의 Public key가 증명서에 저장될 때 연관된 secret private key는 키 소유자의 컴퓨터에 저장되는데, 이 방법은 잘 채택되지 않는다.   * 공격자가 컴퓨터에 대한 접근 권한을 얻으면 그는 쉽게 private key에 접근할 수 있다. * 따라서 private key는 안전하고 제거 가능하며, 암호로 보호된 곳에 접근하는 storage token에 저장된다. * 서로 다른 공급자는 키를 저장하기 위해 서로 다른 storage format을 이용한다. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Hierarchy of CA**   광범위한 네트워크 및 요구 사항 때문에 실질적으로 오직 하나의 CA가 모든 사용자의 디지털 증명서를 발급하는 것은 불가능하다. 따라서 hierarchical certification model이 도입된다.   |  |  | | --- | --- | | Root CA | CA hierarchy의 최상위 CA   * Root CA의 증명서는 self-signed된 증명서이다. | | Root CA 바로 아래의 CA  (그림의 CA1, CA2) | Root CA에 의해 sign된 CA 증명서를 갖는다. | | Subordinate CA의 아래에 있는 CA  (그림의 CA5, CA6) | 더 높은 레벨에 있는 subordinate CA에 의해 sign된 CA 증명서를 갖는다. |  * 증명서의 chain을 verify하는 것은 특정한 증명서 chain이 유효하고, 정확히 sign되었고, 신뢰할 수 있다는 것을 보증하는 것이다. 그 과정은 다음과 같다.  |  | | --- | | 1. 인증된 클라이언트의 디지털 증명서 제공 (보통 증명서 chain에서 위쪽 방향으로) 2. Verifier가 issuer의 public key를 이용하여 그 증명서를 validate한다. 3. Issuer의 증명서를 sign한 상위 CA가 verifier에 의해 증명되었으면 verification은 성공이고 여기서 종료한다. 4. 그렇지 않으면 issuer의 증명서는 클라이언트의 증명서와 유사한 방법으로 verify된다. 이때 verification은 신뢰할 수 있는 CA 또는 Root CA를 찾을 때까지 계속된다. | |