aws re/start

예방: 퍼블릭 키 인프라

Security Fundamentals

보안 수명 주기: 예방 - 퍼블릭 키 인프라를 시작하겠습니다.

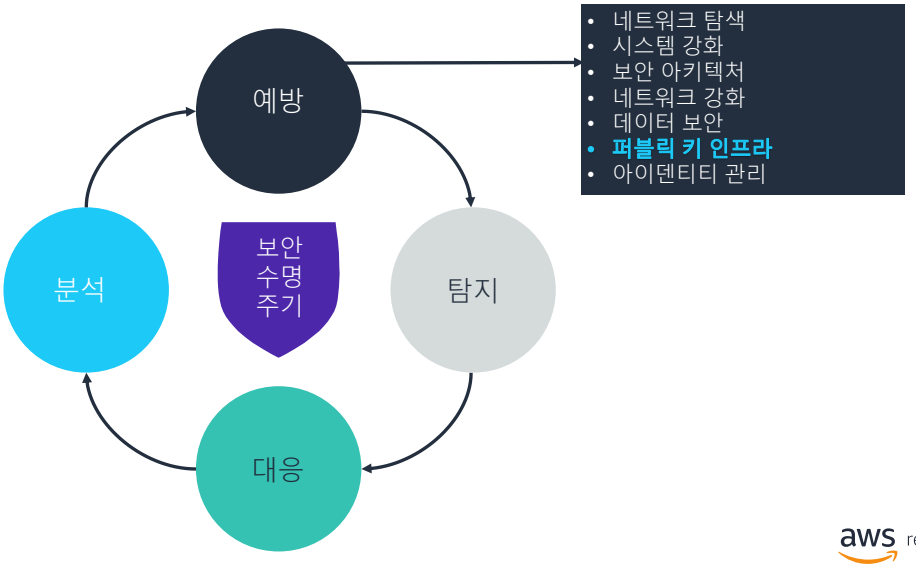
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 퍼블릭 키 인프라(PKI)의 작동 원리과 핵심 구성 요소를 설명합니다.
- 인증서의 작동 원리와 정보 보안에 사용하는 방법을 설명합니다.
- 인증 기관과 일반적인 구성을 설명합니다.

보안 수명 주기: 예방



aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 위협을 탐지했을 때 취해야 할 조치를 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 조치를 구현하면서 주기가 완료됩니다.

이 강의에서는 **퍼블릭 키 인프라(PKI)** 개념과 방법을 예방 단계에 적용하는 방법을 배웁니다.

토론

강사를 신뢰하십니까?

이 질문을 하는 이유는 PKI는 작업을 위해 신뢰에 의존하기 때문입니다. 모든 구성 요소는 엔터티 또는 서버 역할의 형태로 구성된 관계가 있어야 합니다.

강의실을 예로 들어서 AWS가 업무를 수행할 강사를 채용한다고 가정해 봅시다. 학습자가 강사를 신뢰합니까?

PKI가 기술에 적용되면 엔터티는 서버에 액세스하여 안전하게 정보를 검색합니다. 이 서버는 인증서로 보호되는 서버입니다. 엔터티가 연결하는 서버를 신뢰합니까?

퍼블릭 키 인프라

퍼블릭 키 인프라(PKI)는 암호화 기법의 원칙을 적용하는 데 사용되는 기술의 집합입니다.

- 실용적인 키 구현을 기반으로 합니다.
- 이를 통해 다음이 가능합니다.
  - 기밀성, 무결성, 부인 방지, 진본성
  - 신뢰 및 관계 관리

퍼블릭 키 인프라(PKI)는 암호화 기법의 원칙을 적용하는 데 사용되는 기술의 집합입니다. 키의 실용적인 배포와 구현을 기반으로 하며, 기밀성, 무결성, 부인 방지, 진본성을 확보하는 도구 세트가 포함됩니다.

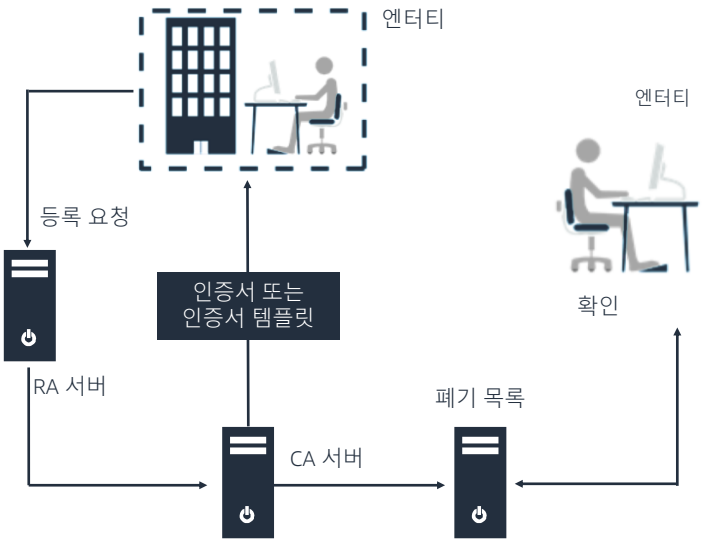
PKI의 구현은 전략적인 프로세스입니다. 이 프로세스는 전역 수준에서 보안과 관련된 위험을 완화하는 것을 목표로 합니다. PKI는 확장 가능하며 다양한 목적으로 사용할 수 있습니다.

대칭 및 비대칭 암호화 기법의 기술적 구현은 PKI를 통해 이루어집니다.

PKI 구성 요소

핵심 구성 요소:

- 인증 기관(CA)
- 인증서
- 폐기 목록
- 등록 기관(RA)
- 엔터티
- 인증서 템플릿



aws re/start

인증 기관

CA에서 엔터티에 **인증서**를 발급하고 신뢰 관계를 관리합니다.

aws re/start

CA는 다음과 같이 다른 유형의 문서를 발행합니다.

- Certificate Practices Statement(CPS) – CA에서 사용하는 관행, 표준, 알고리즘을 설명합니다. CA는 웹 사이트에 이 문서를 게시할 수 있습니다. 여러분은 이 정보를 사용하여 CA가 제공하는 서비스를 비교할 수 있습니다.

- **인증서 정책** - CA의 고객이 따라야 하는 규칙입니다. 이 규칙에는 결제 요구 사항, 허용되는 관행(예: 도박 콘텐츠에 사용할 수 있는지), 인증서 발행이 취소될 수 있는 위반 행위가 포함됩니다. 인증서 발행이 취소되는 위반 행위에는 범죄 행위를 저지르거나 CA에 아이덴티티의 변경 사항을 고지하지 않는 등의 행위가 있습니다.

루트 CA 및 하위 CA

- 루트 CA:
  - 계층 구조의 최상단에 있으며 계층 구조를 초기화함
  - 루트 CA 키를 저장함
  - 격리되어 있으며 오프라인으로 유지됨
  - 엔터티에 서비스를 제공하는 데 직접적으로 관여하지 않음(독립형)
- 하위 CA:
  - **등록 기관**이라고 함
  - 엔터티 요청을 확인하고 검증함
  - 엔터티에 인증서를 발급함

aws re/start

하위 CA는 비교적 작은 환경에서는 요구되지 않습니다. 그러나 PKI 환경을 확대하는 데 더 큰 유연성을 제공합니다.

내부 CA와 외부 CA 비교

특징	내부 CA	외부 CA
구성	조직/회사	제3자
신뢰 수준	조직/회사 내에서만 신뢰함	모든 엔터티가 신뢰함
관리 노력	더 많이 필요함	더 적게 필요함
추가 정보	무료	직접 액세스가 부여되지 않음

보호된 리소스가 외부적으로 게시되지 않으면 내부 CA를 사용할 수 있습니다.

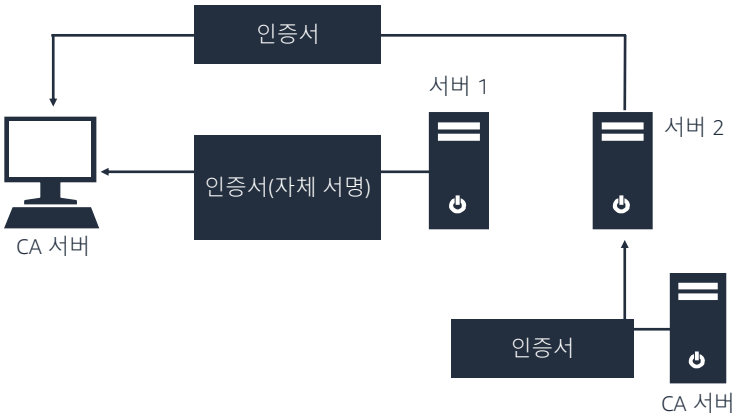
신뢰 형성

신뢰
- 정보를 교환하려는 두 컴퓨터 사이에서 악성 시스템이 통합되는 것을 방지합니다.
- 당사자들의 아이덴티티를 검증하는 퍼블릭 키의 교환을 통해 확보합니다.

퍼블릭 키
- 계층 구조 전체에서 신뢰가 존재하도록 합니다.
- 위치 -
  - 인증서를 요청하는 시스템
  - 서비스를 제공하는 시스템

신뢰는 당사자들의 아이덴티티를 검증하는 퍼블릭 키의 교환을 통해 확보합니다. 퍼블릭 키는 CA가 발행하는 인증서에 연결되어 있습니다.

인증서



aws re/start

디지털 인증서는 네트워크에서 개인, 컴퓨터 및 기타 엔터티의 **온라인 아이덴티티를 나타내는** 데 사용되는 전자 보안 인증 정보입니다. 디지털 인증서를 개인 신분증이라고 생각하면 됩니다.

두 가지 유형의 인증서를 사용할 수 있습니다. **CA가 서명한 인증서**와 **자체 서명된 인증서**입니다.

퍼블릭 키 및 관련 **프라이빗 키**가 있는 인증서는 **암호화**와 **복호화**에 사용할 수 있습니다. 퍼블릭 키만 사용될 경우 인증서는 신뢰를 형성하고 암호화를 수행합니다.

인증서 용례

SSL/TLS:
- 클라이언트와 서버 간에 안전한 인터넷 연결을 구축합니다.
- 예를 들면 신용카드 거래, 데이터 전송, 로그인을 보호하는 데 사용됩니다.
- 디지털 인증서의 프라이빗 키와 퍼블릭 키를 사용하여 데이터를 암호화하고 복호화합니다.

코드 서명:
- 애플리케이션과 스크립트의 진본성을 확인합니다.
- 코드가 서명된 이후에 수정되지 않았음을 보장합니다.
- 디지털 인증서의 프라이빗 키와 퍼블릭 키를 사용하여 디지털 서명 역할을 하고 아이덴티티를 확인합니다.

디지털 인증서는 다음과 같은 용도로 사용할 수 있습니다.

- **보안 소켓 계층(SSL)/전송 계층 보안(TLS)**: 인터넷에서 클라이언트와 서버 간에 보안 연결을 구축하기 위해 SSL/TLS 인증서가 사용됩니다. SSL 인증서는 인증 기관에서 발행하며, 인증서를 요청한 해당 조직에만 사용되는 키 페어(퍼블릭 키와 프라이빗 키)와 연결되어 있습니다.

- **코드 서명**: 코드 서명은 디지털 인증서를 사용하여 소프트웨어의 게시자를 인증하고 코드가 서명된 후에 수정되지 않았음을 보장합니다. 소프트웨어 작성자가 인증서의 프라이빗 키를 사용하여 코드를 서명합니다. 소프트웨어 사용자는 인증서의 퍼블릭 키를 사용하여 작성자의 아이덴티티를 확인합니다.

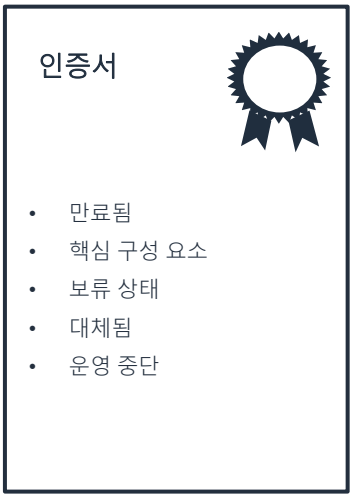
인증서 획득

- **외부** 인증 기관(CA)으로부터 디지털 인증서를 획득하려면 일반적으로 **인증서 서명 요청(CSR)**을 제출해야 합니다.
  - 서버에서 CSR 파일을 만들고 조직에 관한 세부 정보를 제공합니다.
  - CSR 파일을 CA에 전송합니다.
  - CA에게서 디지털 인증서를 받습니다.
  - 인증서를 서버에 설치합니다.
  - 오픈 소스 및 공급 업체별 도구를 사용하여 CSR을 생성할 수 있습니다.
- AWS 클라우드에서는 **AWS Certificate Manager**를 사용하여 상호 작용할 수 있는 **내부** 인증 기관을 제공합니다.

외부 CA로부터 디지털 인증서를 획득하려면 일반적으로 인증서 서명 요청(CSR)을 제출해야 합니다. 오픈 소스 또는 공급 업체별 도구를 사용하여 서버에 CSR을 생성하고 CSR 파일을 CA에 보낼 수 있습니다. 디지털 인증서를 받으면 서버에 설치합니다.

AWS 클라우드에서 **AWS Certificate Manager** 서비스를 사용하여 **내부 AWS Certificate Manager Private Certificate Authority**로부터 인증서를 획득할 수 있습니다.

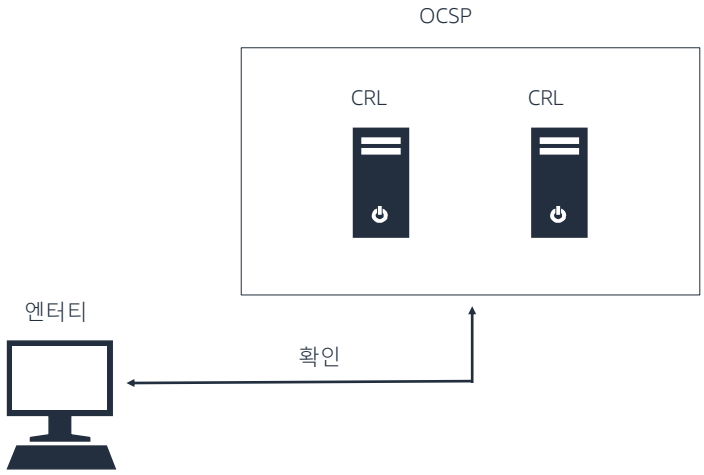
인증서 만료 및 폐기



인증서에는 만료 날짜가 있으며 폐기될 수 있습니다. 만료되거나 폐기된 인증서는 사용할 수 없습니다. 인증서를 발행한 기관에서 유지 관리하는 인증서 폐기 목록(CRL)에 추가되기 때문입니다. 리소스가 인증서를 사용하려고 할 때 이 목록이 확인됩니다.

인증서 폐기 목록

- 더 이상 활성 상태가 아닌 인증서를 나열합니다.
- 주요 고려 사항:
  - 특히 내부 CA를 사용하는 경우 CRL이 액세스 가능해야 합니다.
  - 여러 CRL을 관리하기 위해서는 조직에서 큰 노력이 필요합니다.
  - 기업 환경에 Online Certificate Status Protocol(OCSP)을 사용합니다.

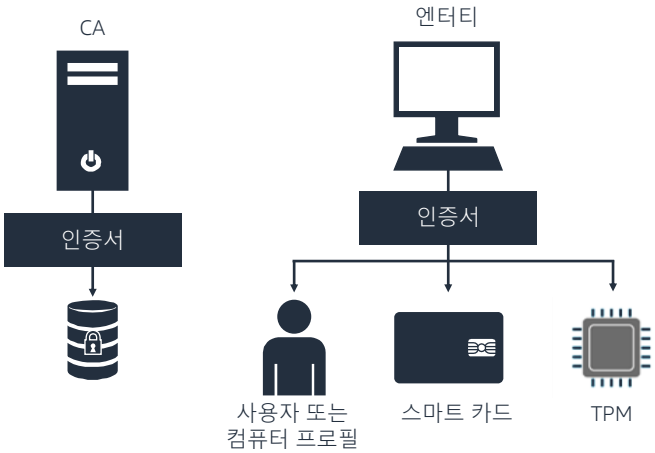


특히 내부 CA에서 인증서를 발행한 경우 CRL이 게시되어야 하고 항상 액세스할 수 있어야 합니다.

Online Certificate Status Protocol(OCSP)은 인터넷 프로토콜입니다. 인증서의 폐기 상태를 검색하는 데 사용됩니다. 기업 환경 내에서 사용됩니다.

인증서 저장

인증서가 작동하려면 안전하게 저장해야 합니다.



aws re/start

기본적으로 인증서는 컴퓨터에 로컬로 저장됩니다. 스마트 카드 또는 신뢰할 수 있는 플랫폼 모듈(TPM) 칩에 저장할 수도 있습니다.

예: Common Access Card(CAC)

aws re/start

Common Access Card(CAC)는 스마트 카드의 한 형태로, 카드의 앞면에 있는 ISO 7816 칩(금색 정사각형)에 정보를 저장합니다. CAC는 일반적으로 군인과 미국 국방부(DoD) 직원이 사용합니다.

ISO 7816 칩에는 여러 인증서를 저장할 수 있습니다. 카드 리더로 ISO 칩을 읽습니다.

CAC는 인증서 외에도 다른 식별 및 액세스 권한 데이터를 저장할 수 있습니다.

CAC는 인증서를 저장하는 것 외에도 다음과 같은 기술을 사용할 수 있습니다.

여러 스토리지 위치 - 정보를 카드 앞면의 옵티컬 영역에 저장하고 카메라로 읽습니다. 카드의 뒷면에 마그네틱 선이 있거나 다른 옵티컬 정보가 저장되어 있을 수 있습니다.

사진 아이덴티티 - 사진 또는 기타 개인 정보가 CAC에 포함되어 소유자를 식별하는 데 사용할 수 있습니다. 따라서 보안 배지로 사용할 수 있습니다.

무선 주파수 식별자(RFID) - 카드 내의 특수한 안테나가 자기장 범위 내에 있을 때 전류를 생성합니다. 이 기능 덕분에 카드에서 근처의 디바이스에 전자 신호를 전송할 수 있습니다. RFID는 보안 영역에 액세스를 허용하기 위해 문의 전자 잠금 장치를 여는 데 흔히 사용됩니다.

핵심 사항

- 퍼블릭 키 인프라(PKI)는 키와 디지털 인증서를 사용하여 리소스를 보호할 수 있도록 하는 원칙과 구성 요소를 정의합니다.
- 디지털 인증서는 개인, 컴퓨터 또는 기타 엔터티의 온라인 아이덴티티를 나타내는 전자 보안 인증 정보입니다.
- 인증 기관(CA)은 인증서를 서명하여 엔터티에 발행하고 신뢰 관계를 관리합니다.
- 디지털 인증서는 자체 서명되거나 CA가 서명할 수 있습니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 퍼블릭 키 인프라(PKI)는 키와 디지털 인증서를 사용하여 리소스를 보호할 수 있도록 하는 원칙과 구성 요소를 정의합니다.
- 디지털 인증서는 개인, 컴퓨터 또는 기타 엔터티의 온라인 아이덴티티를 나타내는 전자 보안 인증 정보입니다.
- 인증 기관(CA)은 인증서를 서명하여 엔터티에 발행하고 신뢰 관계를 관리합니다.
- 디지털 인증서는 자체 서명되거나 CA가 서명할 수 있습니다.