RA 연동 및 권한 관리 정책

문서 개요

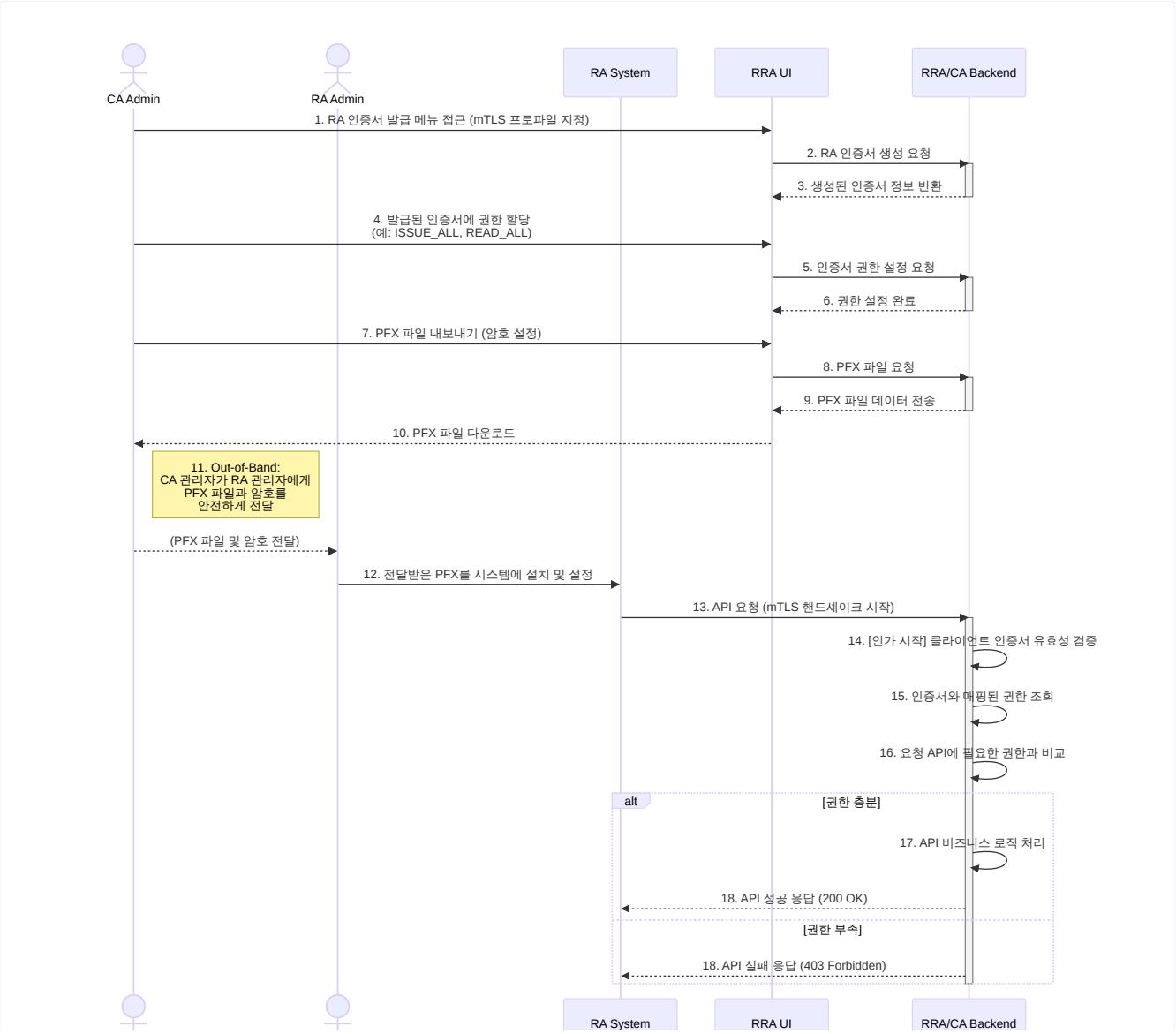
본 문서는 외부 시스템이 등록 기관(RA)으로서 중앙 인증 기관(CA) 시스템과 연동하는 데 필요한 보안 정책 및 기술적 절차를 정의합니다. 주요 목표는 mTLS 기반의 강력한 인증과 인증서에 내재된 권한을 통한 세분화된 인가를 구현하여, 안전하고 통제된 방식으로 RA가 CA의 기능을 사용하도록 하는 것입니다.

핵심 원칙

- **강력한 인증**:
  - 모든 RA와 CA 간의 API 통신은 반드시 mTLS를 통해 이루어져야 합니다. 이를 통해 양측은 서로의 신원을 암호학적으로 검증합니다.
- **인증서 기반 인가**:
  - RA의 API 접근 권한은 RA에게 발급된 클라이언트 인증서 자체에 부여된 권한에 의해 결정됩니다. CA는 API 요청 수신 시, mTLS 세션에서 클라이언트 인증서를 추출하여 해당 인증서가 요청된 작업을 수행할 권한을 가졌는지 확인해야 합니다.
- **최소 권한 원칙**:
  - RA에게는 역할 수행에 필요한 최소한의 권한만 부여해야 합니다. 예를 들어, 인증서 발급 기능만 필요한 RA에게 통계 조회나 다른 인증서를 폐지할 권한을 부여해서는 안 됩니다.
- **안전한 프로비저닝**:
  - RA 시스템을 위한 최초 인증서와 개인키는 안전한 방식으로 전달 및 설치되어야 합니다.

RA 인증서 생명주기 관리

주요 절차 - 시퀀스 다이어그램



Click here to expand...

```
sequenceDiagram
    actor CA Admin
    actor RA Admin
    participant RA System

    %% ================= Part 1: RA 인증서 발급 및 프로비저닝 =================

    CA Admin->>RRA UI: 1. RA 인증서 발급 메뉴 접근 (mTLS 프로파일 지정)
    RRA UI->>RRA/CA Backend: 2. RA 인증서 생성 요청
    activate RRA/CA Backend
    RRA/CA Backend-->>RRA UI: 3. 생성된 인증서 정보 반환
    deactivate RRA/CA Backend

    CA Admin->>RRA UI: 4. 발급된 인증서에 권한 할당<br>(예: ISSUE_ALL, READ_ALL)
    RRA UI->>RRA/CA Backend: 5. 인증서 권한 설정 요청
    activate RRA/CA Backend
    RRA/CA Backend-->>RRA UI: 6. 권한 설정 완료
```

```
    deactivate RRA/CA Backend

    CA Admin->>RRA UI: 7. PFX 파일 내보내기 (암호 설정)
    RRA UI->>RRA/CA Backend: 8. PFX 파일 요청
    activate RRA/CA Backend
    RRA/CA Backend-->>RRA UI: 9. PFX 파일 데이터 전송
    deactivate RRA/CA Backend
    RRA UI-->>CA Admin: 10. PFX 파일 다운로드

    Note right of CA Admin: 11. Out-of-Band: <br>CA 관리자가 RA 관리자에게<br>PFX 파일과 암호를<br>안전하게 전달

    CA Admin-->>RA Admin: (PFX 파일 및 암호 전달)

    RA Admin->>RA System: 12. 전달받은 PFX를 시스템에 설치 및 설정

    %% ================= Part 2: API 통신 및 인가 =================

    RA System->>RRA/CA Backend: 13. API 요청 (mTLS 핸드셰이크 시작)
    activate RRA/CA Backend
    RRA/CA Backend->>RRA/CA Backend: 14. [인가 시작] 클라이언트 인증서 유효성 검증
    RRA/CA Backend->>RRA/CA Backend: 15. 인증서와 매핑된 권한 조회
    RRA/CA Backend->>RRA/CA Backend: 16. 요청 API에 필요한 권한과 비교

    alt 권한 충분
        RRA/CA Backend->>RRA/CA Backend: 17. API 비즈니스 로직 처리
        RRA/CA Backend-->>RA System: 18. API 성공 응답 (200 OK)
    else 권한 부족
        RRA/CA Backend-->>RA System: 18. API 실패 응답 (403 Forbidden)
    end
    deactivate RRA/CA Backend

```

1단계: 발급 및 프로비저닝

RA 시스템이 CA와 통신하기 위한 신원(인증서)을 최초로 확보하는 절차입니다.

- **인증서 발급 요청 (CA 관리자)**
  - CA 관리자는 관리 콘솔(RRA)을 통해 신규 RA 시스템을 위한 종단 인증서(Leaf Certificate) 발급 절차를 시작합니다.
- **인증서 프로파일 및 권한 정의**
  - **프로파일 선택**: 'RA용 TLS 클라이언트 인증서' 프로파일을 선택합니다. 프로파일 구성 예시:
    - **Key Usage**: `Digital Signature`, `Key Encipherment`
    - **Extended Key Usage**: `Client Authentication`
  - **권한 할당**: 해당 RA의 역할에 맞는 권한을 선택하여 인증서에 할당합니다(RA 연동 및 권한 관리 정책 | RA 인증서 기반 권한 정책 상세 참조)
- **인증서 및 키 생성**
  - CA는 요청된 내용에 따라 RA 시스템의 개인키와 공개키 쌍을 생성하고, 해당 공개키로 인증서를 발급합니다.

- **보안 패키징**
  - CA는 발급된 RA 인증서와 암호화된 개인키를 하나의 파일로 패키징합니다.
  - **포맷**: PKCS#12 (`.pfx` , `.p12`)
  - **암호화**: 패키지 파일은 강력한 암호로 보호되어야 합니다.
- **안전한 전달 (Out-of-Band)**
  - 생성된 `.pfx` 파일과 해당 파일의 암호는 RA 시스템 관리자에게 **별도의 안전한 채널**을 통해 전달되어야 합니다 (예: 암호화된 이메일, 보안 메신저 등).
- **RA 시스템 설정**
  - RA 관리자는 전달받은 `.pfx` 파일을 RA 시스템에 설치하고, CA와 통신 시 해당 인증서를 사용하도록 mTLS 클라이언트를 설정합니다.

2단계: 통신 및 인가

RA가 CA의 API를 호출하는 런타임 절차입니다.

1. **mTLS 세션 수립**
   - RA 클라이언트는 CA의 API 엔드포인트로 mTLS 연결을 시도하며, 이때 1단계에서 발급받은 자신의 인증서를 제시합니다.
   - CA 서버는 제시된 RA 인증서의 유효성(신뢰 체인, 유효 기간 등)을 검증하고 세션을 수립합니다.
2. **인증서 추출 및 권한 확인**
   - CA의 API 게이트웨이 또는 Spring Security와 같은 보안 계층은 수립된 mTLS 세션에서 RA 클라이언트의 인증서를 추출합니다.
   - CA는 추출된 인증서의 고유 정보(예: Serial Number, Subject Key Identifier)를 기반으로, 해당 인증서에 부여된 권한 목록을 내부 데이터베이스 또는 인증서 확장(Custom Extension)에서 조회합니다.
3. **API 접근 제어**
   - CA는 조회된 권한 목록과 RA가 호출한 API 엔드포인트에 필요한 권한을 비교합니다.
   - 권한이 충분한 경우, API 요청 처리를 허용합니다.
   - 권한이 없는 경우, `403 Forbidden` 오류를 반환합니다.
   - 모든 API 접근 시도는 감사 로그(Audit Log)에 기록되어야 합니다.

3단계: 갱신

만료가 임박한 RA 인증서를 새로운 인증서로 교체하는 절차입니다.

- RA 시스템은 현재 유효한 인증서를 사용하여, 자신의 인증서를 갱신하기 위한 API(`RENEW_SELF` 권한 필요)를 호출합니다.

- CA는 갱신 요청을 한 인증서가 유효하고 `RENEW_SELF` 권한을 가졌는지 확인한 후, 동일한 정보와 권한을 가진 새로운 유효 기간의 인증서를 발급하여 반환합니다.
- RA 시스템은 응답으로 받은 새 인증서를 기존 인증서와 교체 설치합니다.

4단계: 폐지

RA 인증서의 키가 유출되거나 더 이상 사용되지 않을 때 인증서를 무효화하는 절차입니다.

- **즉시 폐지**: RA 시스템의 보안 침해가 의심되는 경우, CA 관리자는 즉시 관리 콘솔을 통해 해당 RA 인증서를 폐지해야 합니다.
- **CRL/OCSP 게시**: 폐지 정보는 즉시 CRL(인증서 폐지 목록)에 추가되고 OCSP(온라인 인증서 상태 프로토콜) 응답에 반영되어야 합니다.
- **상태 확인**: CA 서버는 mTLS 세션 수립 시, 클라이언트가 제시한 RA 인증서가 폐지되지 않았는지 CRL/OCSP를 통해 반드시 확인해야 합니다.

RA 인증서 기반 권한 정책 상세

RA 인증서에 부여할 수 있는 권한의 종류와 설명은 PV25 권한관리 | Certificate 당 권한 참조하세요.

보안 고려사항

- **PFX 파일 보안**: 최초 발급된 `.pfx` 파일과 암호는 매우 중요한 자산입니다. 전달 과정의 보안을 철저히 하고, 전달 완료 후에는 CA 시스템에서 해당 파일을 영구 삭제하는 것을 권장합니다.
  - 유저 가이드 작성시 반드시 상기 내용을 포함시켜야 합니다.
- **RA 개인키 보호**: RA 시스템은 설치된 인증서의 개인키를 운영체제 수준의 접근 제어, HSM 등을 통해 안전하게 보호해야 할 책임이 있습니다.
- **감사 로그**: CA는 어떤 RA가 언제, 어떤 API를 호출했으며, 그 결과가 성공이었는지 실패였는지 모두 기록하여 비정상적인 활동을 추적할 수 있어야 합니다.