

기밀연산 인공위성 시스템 적용

종합설계 6회차

11조 - 조민성, 신희성, 김주호

지도교수 - 장진수 교수님

Table of contents

01

유스케이스 선정

02

다이어그램

03

키 생성

04

키 교환

05

키 저장

핵심 기술

1. OP-TEE(Trusted Execution Environment) 환경

- 하드웨어 기반 신뢰 환경
- 데이터 저장 보안 강화

2. PQC(Post-Quantum Cryptography) 알고리즘

- 양자 이후 암호 알고리즘
- 데이터 통신 보안 강화

01. 유스케이스 선정

유스케이스

1. 키 생성

- 대칭키 기반의 디지털 서명 방식을 통한 보안

2. 키 교환

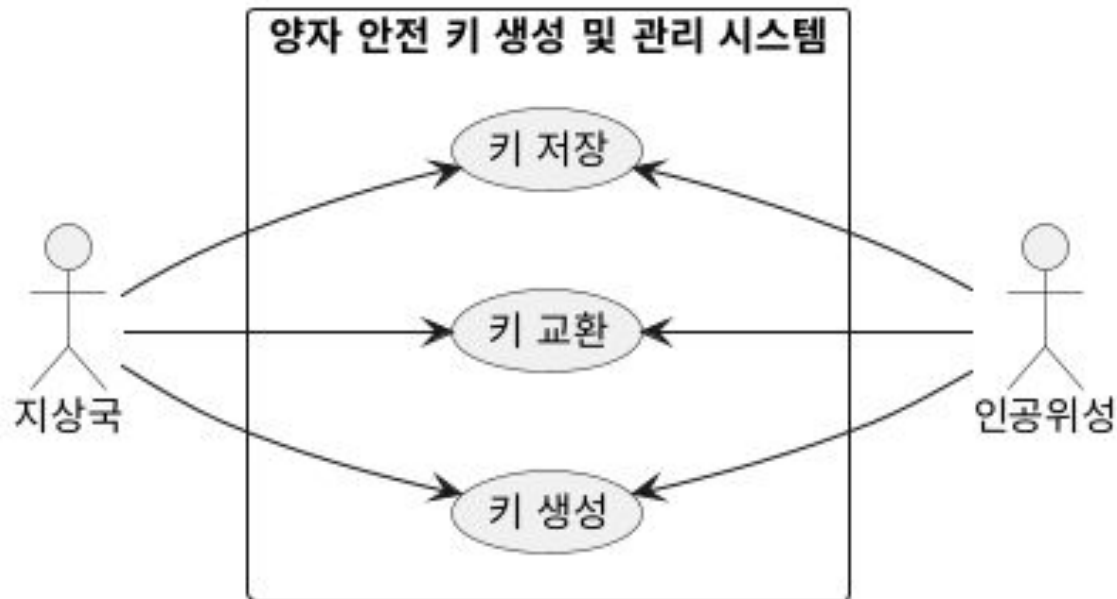
- **PQC** 알고리즘을 통한 암호화 데이터 통신

3. 키 저장

- **OP-TEE** 환경을 사용해 보안 강화된 데이터 저장

02. 다이어그램

유스케이스 다이어그램



Instruction



설명

키 교환을 위해 지상국에서 키를 생성하는 과정



조건

사전 조건

- 지상국 시스템 부팅 완료, OP-TEE 및 TA 작동, RNG(난수 생성기) 사용 가능

사후 조건

- 유효한 public/private Key 쌍이 생성
- private Key가 Secure Storage에 저장
- public Key가 키 교환용으로 준비

Process

- 1) 사용자는 CA에서 TA에게 key쌍을 생성하도록 요청
- 2) TA에서 PQC 알고리즘으로 key쌍 생성
 - 2-1) RNG 동작 실패 시 에러를 반환 후 재시도 요청
- 3) private Key를 Secure Storage에 저장
 - 3-1) Secure Storage 접근에 실패 시 로그 기록 후 처리
- 4) public Key를 CA로 반환

03. 키 교환

Instruction



설명

키 교환을 위해 지상국에서 인공위성으로의 요청 과정



조건

사전 조건

- 양측 모두 public/private 키 쌍을 보유

사후 조건

- 공유 비밀 키가 계산되어 TEE에 저장

03. 키 교환

Process

- 1) 지상국과 인공위성은 각각 자신의 공개키를 **REE**를 통해 전송
1-1) 통신이 끊기거나 오류가 발생할 경우 키 교환 실패 메시지 전송
- 2) 수신 측은 상대방의 공개키를 받아 **TEE**로 전달
- 3) 수신한 공개키와 자신의 비밀키를 조합하여 공유 비밀키 계산
- 4) 계산된 공유 키는 **TEE**의 **secure storage**에 저장

03. 키 저장

Instruction



설명

OP-TEE에 키를 저장하는 과정



조건

사전 조건

- 생성 또는 교환된 키가 메모리에 존재

사후 조건

- 키가 OP-TEE의 **secure storage**에 안전하게 저장

Process

- 1) 시스템은 키 생성 또는 교환 직후 키를 **secure storage**에 저장
 - 1-1) 저장 공간 부족 또는 저장 중 예외 발생 시 오류 메시지를 리턴
 - 1-2) 반복 실패 시 관리자 개입 필요
- 2) **OP-TEE**에서 제공하는 **API**를 통해 저장하고 접근 권한은 제한
- 3) 저장 성공 여부를 로그로 기록하고 **Actor**에게 전송

출처

Thanks!

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons, infographics & images by [Freepik](#)

https://github.com/isord/satellite_OPTEE/tree/week3