# 기밀연산 인공위성 시스템 적용

종합설계 11회차

11조 - 조민성, 신희성, 김주호 지도교수 - 장진수 교수님

#### **Table of contents**

01 02 03

테스트 계획

테스트 상세

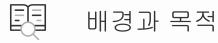
테스트 관리

04 \_\_\_\_\_\_ 05

테스트 케이스

테스트 케이스 환경

### 테스트 계획



양자컴퓨터 환경에서 PQC로 외부 공격 차단 OP-TEE를 통한 안전한 키 저장 및 교환



- 테스트 항목
- 1. TEE 정상 동작 확인
- 2. PQC 키 생성, 교환 기능
- 3. 키 저장 후 접근 제어 기능

#### 테스트 상세



제외 항목

실제 위성 하드웨어/우주 환경 테스트 제외 양자 컴퓨터 공격 시뮬 제외 스트레스/ 부하 테스트 제외



테스트 방법 및 P/F 기준

- 1. 단위 테스트 (기능별 PQC, TEE): PQC, TEE 정상 작동 확인
- 2. 시스템 테스트 (전체 흐름 검증): 시스템 요구사항 명세서의 모든 기능 수행
- 3. 블랙박스 테스트: TEE가 아닌 환경에서 키에 접근 제한
- 4. 리그레션 테스트: 시스템 오류 및 예외상황 확인

#### 테스트 관리

작업 절차

- 1. 테스트 계획 수립
- 2. 요구사항/기능 명세 검토
- 3. 테스트 케이스 작성 및 검토
- 4. 테스트 수행 및 결함 수정
- 5. 블랙박스/리그레션 테스트 진행
- 6. 테스트 결과 보고 및 종료



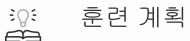
기술 자원

OP-TEE가 구축된 OS 커널 가상의 키 위성통신을 대체할 수신 장비

### 테스트 관리

인력 자원

- 1. OS를 설치하고 테스트 키를 만들 수 있는 IT 인력
- 2. 통신망을 구축하고 키 교환을 수행할 수 있는 인력
- 3. 테스트 전문가



테스트 인력 대상 간단한 테스트 교육 실시

### 테스트 관리

일정

OP-TEE 구축 및 환경 준비 : 약 2주

이후 기능 별 테스트 및 통합 시나리오 검증

☆ 리스크 및 대응

환경 구충에 시간이 걸릴 수 있으므로 단계적 점검 후 테스트를 진행

02. 테스트 케이스

## 테스트 범위

테스트 범위

1. OP-TEE 기반 TEE 내의 PQC 키 저장 모듈

2. REE에서의 PQC 키 교환 요청 처리

3. 지상국 인공위성 간의 전체 시나리오 흐름 테스트

#### 02. 테스트 케이스

## 테스트 케이스 명세

|  | Id   | 테스트 대상              | 테스트 조건   | 테스트 데이터   | 예상 결과  |
|--|------|---------------------|--|---|--|
|  | TC-1 | PQC 키 생성            | 지상국에서 키 요청   | N/A   | PQC 공개키/개인키 쌍<br>생성 성공   |
|  | TC-2 | 키 교환 요청             | REE -> TEE 전송                                      | 공개키 데이터   | 공개키 수신, TEE 내 저장<br>성공   |
|  | TC-3 | 키 저장                | TEE 내부 저장 동작                                       | PQC 키 데이터   | TEE 내 Secure Storage에<br>기록 확인   |
|  | TC-4 | 접근 제어               | REE에서 TEE 키 접근 시도                                  | 비인가 접근  | 접근 거부, 로그 기록 됨   |
|  | TC-5 | 통신 시나리오             | 지상국 <-> 위성 간 시나리오                                  | 전체 키 교환 흐름  | 성공적인 키 교환 후 저장   |
|  |      | TC-1 TC-2 TC-3 TC-4 | TC-1 PQC 키 생성  TC-2 키 교환 요청  TC-3 키 저장  TC-4 접근 제어 | TC-1     PQC 키 생성     지상국에서 키 요청       TC-2     키 교환 요청     REE -> TEE 전송       TC-3     키 저장     TEE 내부 저장 동작       TC-4     접근 제어     REE에서 TEE 키 접근 시도 | TC-1     PQC 키 생성     지상국에서 키 요청     N/A       TC-2     키 교환 요청     REE -> TEE 전송     공개키 데이터       TC-3     키 저장     TEE 내부 저장 동작     PQC 키 데이터       TC-4     접근 제어     REE에서 TEE 키 접근 시도     비인가 접근 |

02. 테스트 케이스

### 테스트 케이스 환경

테스트 환경

QEMU 기반 OP-TEE 시뮬레이터 Ubuntu 22.04 LTS 개발 환경

클라이언트-서버 시리얼 통신 시뮬레이터

PQC 라이브러리 (CRYSTALS-KYBER)



테스트 절차 제약사항

OP-TEE 빌드 및 환경 구성 완료 필수

Secure Storage 정상 작동 여부 선확인

지상국/위성 시뮬레이션 테스트 코드 준비



# Thanks!

CREDITS: This presentation template was created by <u>Slidesgo</u>, and includes icons, infographics & images by <u>Freepik</u>

https://github.com/isord/satellite\_OPTEE/tree/week11