Usecase Specification Document

Project Name	기밀연산 인공위성 시스템 적용 (PQC 기반 보안 키 교환 및 OP-TEE 저장)

11 조

202002558 조민성
201902711 신희성
201802076 김주호

지도교수: 장진수 교수님 (서명)

Document Revision History

Rev#	Date	Affected Section	Author
1	2025/04/12	유스케이스 초안 작성	조민성 신희성 김주호

Table of Contents

List of Figure

1. Introduction

1.1. Objective

이 문서는 기밀 연산 기반 인공위성 보안 시스템의 요구사항을 정의하고, 시스템이 제공해야 할 주요 기능을 명확히 설명하는 것을 목적으로 한다. 본 시스템은 Post-Quantum Cryptography(PQC) 기반의 키 교환 기술과 OP-TEE(Trusted Execution Environment) 기반의 보안 저장 기술을 결합하여, 보다 높은 수준의 위성 보안 체계를 구현한다. 또한, 각 기능에 대해 상세한 설명과 유스케이스 다이어그램 및 유스케이스 명세서를 포함하여 전체 시스템의 동작 흐름과 사용자 상호작용을 구조적으로 기술한다.

2.Usecase Diagram

2.1. 설정 Diagram

위성과 키 교환을 수행하는 프로그램의 서브시스템에 대한 유스케이스 다이어그램은 다음과 같다.

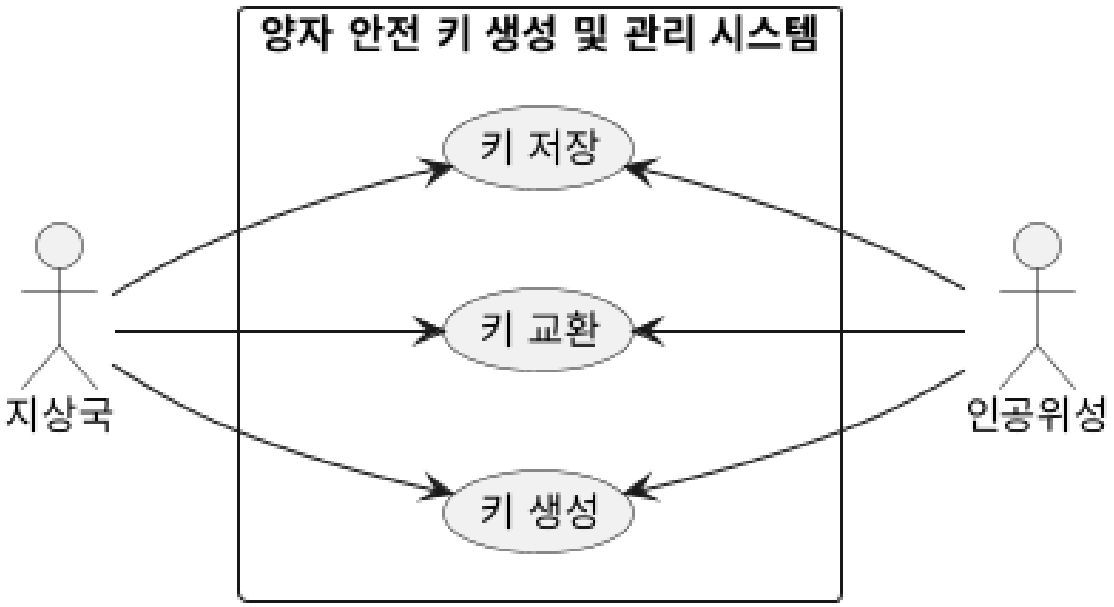

그림 1. 서브시스템에 대한 유스케이스 다이어그램

3.Usecase Specification

3.1. 키 생성

Usecase 이름	키 생성
ID	001
간략 설명	키 교환을 위해 지상국에서 키를 생성하는 과정을 설명한다.
Actor	Client(Initiator), Satellite
Pre-Conditions	- 지상국 시스템 부팅 완료. OP-TEE 및 TA 작동. RNG(난수 생성기) 사용 가능.
Main Flow	1) 사용자는 CA에서 TA에게 key쌍(public Key/private Key)을 생성하도록 요청. 2) TA에서 PQC 알고리즘으로 key쌍 생성. 3) private Key를 Secure Storage에 저장. 4) public Key를 CA로 반환.
Post-Conditions	- 유효한 public/private key쌍이 생성됨. - private Key가 Secure Storage에 저장됨. - public Key가 키 교환용으로 준비됨.
Alternative Flow	2-1) RNG 동작이 실패하였다. 에러를 반환하고 재시도 요청하여, 다시 수행한다. 3-1) Secure Storage 접근에 실패하였다. 로그 기록을 하고, 실패 처리로 한다.

3.2. 키 교환

Usecase 이름	키 교환
ID	002
간략 설명	키 교환을 위해 지상국에서 인공위성으로의 요청 과정을 설명한다.
Actor	Client(Initiator), Satellite
Pre-Conditions	- 양측 모두 public/private 키 쌍을 보유하고 있어야 함
Main Flow	1) 지상국과 인공위성은 각각 자신의 공개키를 REE를 통해 전송한다. 2) 수신 측은 상대방의 공개키를 받아 TEE로 전달한다. 3) TEE 내부에서는 수신한 공개키와 자신의 비밀키를 조합하여 공유 비밀키를 계산한다. 4) 계산된 공유 키는 TEE의 secure storage에 저장된다.
Post-Conditions	- 공유 비밀 키가 계산되어 TEE에 저장됨
Alternative Flow	1-1) 공개키 전송 도중 통신이 끊기거나 오류가 발생할 경우 키 교환 실패 메시지를 전송하며, 재시도 로직이 작동됨.

3.3. 키 저장

Usecase 이름	키 저장
ID	003
간략 설명	OP-TEE에 키를 저장하는 과정을 설명한다
Actor	Client(Initiator), Satellite
Pre-Conditions	- 생성 또는 교환된 키가 메모리에 존재해야 한다

Main Flow	1) 시스템은 키 생성 또는 교환 직후, 키를 secure storage에 저장한다. 2) 저장은 OP-TEE에서 제공하는 API를 통해 이루어지며, 접근 권한은 제한된다. 3) 저장 성공 여부를 로그로 기록하고 액터에게 알린다.
Post-Conditions	- 키가 OP-TEE의 secure storage에 안전하게 저장된다.
Alternative Flow	1-1) 저장 공간 부족 또는 저장 중 예외 발생 시 오류 메시지를 리턴하고, 재시도를 시도함. 1-2) 반복 실패 시 관리자 개입 필요.

4.AI 도구 활용 정보

사용 도구	*GPT-4o*
사용 목적	*그림자료 생성 (Usecase diagram code 생성)*
프롬프트	• *위 내용의 유스케이스를 다이어그램으로 만들 code 생성해줘* • *유스케이스에 사용할 개요 초안을 작성해줘*
반영 위치	*1. 유스케이스 다이어그램 그림 (p.5)* *2. 프로젝트 주제에 맞는 유스케이스 정리해줘 (p.7)*
수작업 수정	*있음(오타 수정, 잘못된 정보 수정, 다이어그램 수정을 위한 code 수정 등)*