국가용 보안요구사항 V3.0 기반의

국내용 보안목표명세서 작성 템플릿 V1.0

2025. 4. 11.

과학기술정보통신부

IT보안인증사무국

• 제·개정 이력

버전	일 자	변경 내용
1.0	2025. 4. 11	ㅇ 국가용 보안요구사항 V3.0 기반의 국내용 보안 목표명세서 작성 템플릿 제정

서 문

2024년 과학기술정보통신부는
정보보호제품 평가·인증 제도의 개선을 통해 기업의 참여 확대와 평가·인증 준비의 실효성을 제고하고자
다양한 정책적 노력을 추진하였습니다.

이에 발맞춰 IT보안인증사무국은
기업이 정보보호제품 평가를 준비하는 과정에서 겪는 어려움을 덜어주기 위해
제출문서에 대한 가이드와 템플릿을 제공하고, 작성 샘플을 마련하여 실질적인 지원을 제공하고자 합니다.

본 가이드는 정보보호제품 CC 평가 시 요구되는 중요 제출문서인 보안목표명세서 평가에서의
복잡한 절차와 기술적 요건을 명확히 이해할 수 있도록 구체적인 지침과 사례를 제시하여,
문서의 구성별(세부목차별) 작성 방향에 대한 안내와 함께 실무적인 작성 예시를 포함하고 있습니다.

본 가이드를 통해 기업이 평가를 준비하는 과정에서부터 체계적이고 효율적으로
평가·인증에 대한 사전 역량을 강화할 수 있을 것으로 기대합니다.

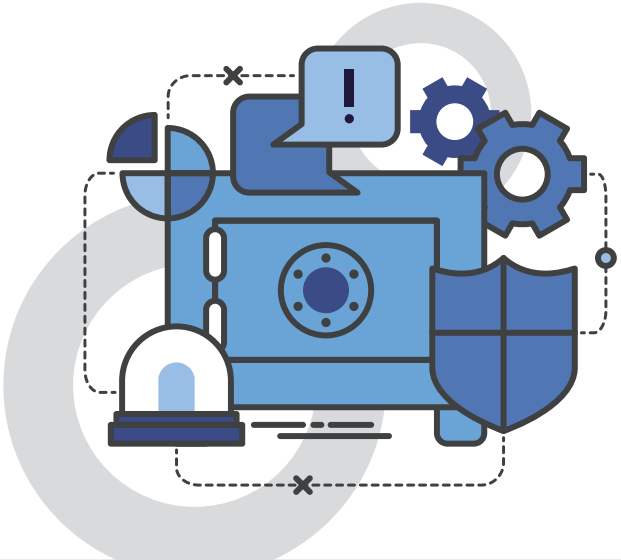
CONTENTS

06 보안요구사항

07 TOE 요약명세

08 참고자료

09 용어 및 약어



01

보안목표명세서 소개

1. 보안목표명세서 소개

1.1. 보안목표명세서 참조

제 목	
버 전	
작성자	
발간일	

1.2. TOE 참조

☞ TOE 버전 및 TOE 구성요소 식별 방법 및 서술은 최신의 '정보보호제품 평가•인증 해설서' 참조하시기 바랍니다.

TOE 명칭		XXX
TOE 버전		Vx.x
TOE 구성요소	HW	XXX (☞ TOE 유형이 하드웨어 일체형인 경우 SW가 설치되는 하드웨어 모델명)
	SW	XXX Vx.x (빌드버전 : x.x.xxxx.x)
	문서	XXX 설치매뉴얼 Vx.x XXX 운영매뉴얼 Vx.x

1.3. TOE 개요

☞ TOE 유형, TOE 용도 및 주요 보안특성을 요약하여 서술

1.3.1. TOE의 용도 및 주요 보안 특성

☞ TOE가 보안과 관련하여 어떤 기능을 제공하며 어떠한 운영환경에서 어떠한 목적으로 사용할 수 있는지에 대해 전반적인 사항을 간단 명료하게 서술

☞ TOE를 포함한 제품이 제공하는 모든 보안특징을 서술하고 평가범위와 평가범위 이외의 부분을 명확하게 식별

1.3.2. TOE 유형

☞ 국내용 평가제품인 경우 국가용 보안요구사항에 해당하는 제품 유형을 식별하고 핵심 기능 및 운영환경을 요약 서술

1.3.3. 비-TOE 식별(하드웨어/소프트웨어/펌웨어)

☞ TOE 범위에 포함되지 않은 IT 자원이나 TOE의 정상 동작을 위해 필요한 최소한의 IT자원을 식별

☞ TOE가 외부 IT 실체와 상호작용을 통해 동작을 수행하는 경우, 아래와 같이 외부 IT 실체와 관련된 사항을 작성, 외부 IT 실체의 예로는 NTP, SYSLOG, SNMP, SMTP 등이 있음

TOE 구성요소	하드웨어 플랫폼	운영체제	기타 SW
	•	•	•
	•	•	•
	•	•	•
	•	•	•
	•	•	•

외부 IT 실체	용도
Syslog 서버	•
NTP 서버	•

1.4. TOE 설명

1.4.1. TOE 물리적 범위

(가) TOE 구성요소 및 배포 방법

☞ TOE를 구성하는 모든 하드웨어, 펌웨어, 소프트웨어, 설명서 등을 식별(파일명 포함)하여 목록 작성

☞ TOE 구성요소마다 배포형태와 배포방법을 서술

☞ 하드웨어 모델 사양과 관련된 사항은 최신 '정보보호제품 평가·인증 해설서'의 '하드웨어 일체형 장비의 확장 모델 서술 및 평가 방안'을 참고, 또한 TOE가 하드웨어 일체형 장비 형태의 제품인 경우,NIC, HDD, Memory, 보안기능 수행 하드웨어(예: 암호가속기 등)는 확장할 수 있으며 그 밖의 하드웨어(예: CPU)는 확장 구성이 허용되지 않음에 유의

TOE 구성요소	버전정보	배포 형태	배포 방식

제3자 요소(버전 포함)	보안기능 세부 설명

(나) TOE 운영환경

☞ 일반적인 TOE 설치 및 운영환경을 고려하여 시스템 구성 및 네트워크 구성도 작성

TOE 운영환경

(시스템 구성 및 네트워크 구성도)

1.4.2. TOE 논리적 범위

☞ TOE가 제공하는 보안특징을 CC 제2부의 보안기능 클래스 단위로 구분하여 서술

(가) 보안감사

(나) 암호지원

(다) 사용자 데이터 보호

(라) 식별 및 인증

(마) 보안관리

(바) TSF 보호

(사) TOE 접근

(아) 안전한 경로/채널

02

준수 선언

2. 준수 선언

2.1. 공통평가기준 준수 선언

공통평가기준		정보보호시스템 공통평가기준 버전 3.1 개정 2판 •정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1R1, 2006. 9., CCMB-2006-09-001 •정보보호시스템 공통평가기준 2부 : 보안기능요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-002 •정보보호시스템 공통평가기준 3부 : 보증요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-003
준수 형태	2부 보안기능요구사항	
	3부 보증요구사항	
	패키지	

2.2. 보호프로파일(보안요구사항), 패키지 준수 선언

☞ 최신 국가용 보안요구사항 및 사전 인증이 필요한 제품 유형은 국가정보원(nis.go.kr) 또는 국가사이버안보센터(ncsc.go.kr) 웹사이트를 참고

보호프로파일(보안요구사항)	-
보증등급	-
TOE 유형	-

2.3. 준수 선언의 이론적 근거

본 보안목표명세서에서는 보호프로파일을 준수선언하지 않았으므로 해당사항이 없다.

03

보안문제정의

3. 보안문제정의

3.1. 위협

위협원은 보호하고자 하는 자산에 비인가 된 접근 또는 비정상적인 방법으로 위해를 가하는 IT실체 및 사용인이며, 다음과 같은 다양한 위협을 발생시킬 수 있다. 이때 TOE에 대한 위협원은 강화된-기본 수준의 전문지식, 자원, 동기를 가진다.

☞ 평가보증등급을 고려하여 위협원의 수준 명시

☞ TOE 용도, TOE 운영환경, TOE 논리적 범위를 고려하여 TOE가 대응해야 하는 위협과 더불어 TOE 자체에 대한 위협을 모두 고려하여 명세

3.1.1. 비인가 된 접속

T.	(T.)
T.	(T.)
T.	(T.)
T.	(T.)
T.	(T.)

3.1.2. 정보유출

T.	(T.)
T.	(T.)

3.1.3. ooo

☞ 일반적인 “비인가된 접속” 및 “정보유출” 위협 유형 이외에 TOE 유형 및 용도를 고려하여 추가 위협 유형에 대해 서술

T.	(T.)
T.	(T.)
T.	(T.)

3.2. 조직의 보안정책

☞ TOE에서 다루고자 하는 보안특성 및 범위를 정의한 것으로 TOE 및 TOE 운영환경에서 준수해야하는 보안정책을 명세

P.	(P.)
P.	(P.)

3.3. TOE 운영환경에 관한 가정사항

☞ TOE 운영환경에 관한 가정사항은 TOE 범위와 연관있으며 TOE가 직접적으로 대응할 수 없는 사항에 대해 명세하거나 TOE가 설치 운영되는 일반적인 운영환경을 명세

A.	(A.)
A.	(A.)

04

보안목적

4. 보안목적

4.1. TOE 보안목적

☞ 보안문제정의(위협, 조직의 보안정책)와 SFR 사이의 연결고리를 만들도록 SFR을 자연어로 표현한 보안목적을 명세

O.	O.
O.	O.

4.2. 운영환경에 대한 보안목적

☞ 위협, 조직의 보안정책, 가정사항에 대응되나 TOE에서 제공하지 못하는 사항에 대해 명세

OE	OE.
OE	OE.
OE	OE.

4.3. 보안목적의 이론적 근거

4.3.1. TOE 보안목적의 이론적 근거

(가) TOE 보안목적과 SPD 간 일치성 분석

	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.
T.														
T.														
T.														
T.														
P.														
P.														
P.														
P.														

[TOE 보안문제정의와 TOE 보안목적 대응]

(나) TOE 보안목적과 SPD 간 추적성 입증

☞ TOE 보안목적의 어떤 보안기능성이 위협의 어떤 부분을 대응(제거, 감소, 완화)하는지 관점에서 ST 작성자/개발자의 의도를 서술

T.	O.
T.	O.
T.	O.
T.	O.
T.	O.

4.3.2. 운영환경에 대한 보안목적의 이론적 근거

(가) 운영환경에 대한 보안목적과 SPD 간 일치성 분석

☞ 일치성 분석 표에서 매핑되지 않는 SPD 또는 운영환경에 대한 보안목적이 존재하는 경우 일치성이 결여된 것이므로 SPD 또는 운영환경에 대한 보안목적을 을 추가 식별하여 명세하거나 기존의 내용을 보완해야 함

	OE.	OE.	OE.	OE.	OE.	OE.	OE.
P.							
P.							
A.							
A.							
A.							
A.							

[TOE 보안문제정의와 운영환경에 대한 보안목적 대응]

(나) 운영환경에 대한 보안목적과 SPD 간 추적성 입증

☞ 각 운영환경에 대한 보안목적은 최소 1개 이상의 위협, 조직의 보안정책 또는 가정사항으로 추적됨을 입증

A.	OE.

A.	OE.

05

확장 컴포넌트 정의

5. 확장 컴포넌트 정의

본 보안목표명세서에서 확장한 컴포넌트의 정의는 다음과 같다.

☞ 확장컴포넌트가 존재하지 않은 경우 “본 보안목표명세서에서 확장한 컴포넌트는 없다.”로 서술

☞ CC 제2부 또는 CC 제3부의 표현형식에 따라 필요한 단위(클래스, 패밀리, 컴포넌트)로 확장 정의

5.1. 클래스 명(FXX, XXXXXX)

5.1.1. 패밀리 명

패밀리 개요

컴포넌트 계층관계 및 설명

관리 : 컴포넌트 1, 컴포넌트 2

FMT에서 다음과 같은 관리 기능이 고려될 수 있다.

a)

감사 : 컴포넌트 1

FAU_GEN 보안감사 생성 데이터 생성 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사 기록할 것을 권고한다.

a)감사수준 :

b)최소 :

(가) 컴포넌트 .X 컴포넌트 명

계층관계	없음
종속관계	
엘리먼트.X.1	TSF는 ~~해야 한다.
엘리먼트.X.2	TSF는 ~~해야 한다.
엘리먼트.X.3	TSF는 ~~해야 한다.
엘리먼트.X.4	TSF는 ~~해야 한다.
엘리먼트.X.5	TSF는 ~~해야 한다.

06

보안요구사항

6. 보안요구사항

본 보안목표명세서는 일부 약어 및 명확한 의미 전달을 위해 영어를 혼용한다. 사용된 표기법, 형태, 작성 규칙은 공통평가기준을 따른다.

공통평가기준은 보안기능요구사항에서 수행될 수 있는 반복, 할당, 선택, 정교화 오퍼레이션을 허용한다. 각 오퍼레이션은 본 보안목표명세서에서 사용된다.

반복

오퍼레이션을 다양하게 적용하여 하나의 컴포넌트를 여러 번 반복할 경우 사용된다. 반복 오퍼레이션의 결과는 컴포넌트 식별자 뒤에 괄호 안의 반복번호, 즉. (반복 번호)로 표시한다.

할당

명세되지 않은 매개변수에 특정 값을 할당하는데 사용된다(예 : 패스워드 길이). 할당 오퍼레이션의 결과는 대괄호, 즉. [할당 값]으로 표시된다.

선택

요구사항 서술시 정보보호시스템 공통평가기준에서 제공되는 선택사항 중 하나 이상을 선택하는데 사용된다. 선택 오퍼레이션의 결과는 *밑줄 그은 이탤릭체*로 표시된다.

정교화

요구사항에 상세사항을 추가함으로써 요구사항을 더욱 제한하는데 사용된다. 정교화 오퍼레이션의 결과는 굵은 글씨로 표시된다.

본 보안목표명세서는 요구사항의 의미를 명확히 하고, CC 컴포넌트 오퍼레이션 적용에 대한 ST 작성자의 의도를 전달하기 위해 “ST 작성자 註”가 제공된다.

6.1. 보안기능요구사항

TOE가 만족하는 보안기능요구사항은 다음과 같다. '정교화', '반복' 오퍼레이션이 적용된 컴포넌트에 대해 비고란에 해당 사항을 기재한다.

보안기능 클래스	보안기능 컴포넌트		비고 (정교화, 반복 구분)
보안감사 (FAU)	FAU_GEN.1	감사데이터 생성	
암호지원 (FCS)	FCS_CKM.1(1)	암호키 생성(SSH 관리접속)	
사용자 데이터보호 (FDP)	FDP_IFC.2(1)	완전한 정보흐름 통제(침입차단)	
식별 및 인증 (FIA)	FIA_AFL.1(1)	인증 실패 처리(패스워드 기반 관리자 인증)	
보안관리 (FMT)	FMT_MOF.1	보안기능 관리	
TSF 보호 (FPT)	FPT_STM.1	신뢰할 수 있는 타임스탬프	
TOE 접근 (FTA)	FTA_MCS.2	사용자 속성별 동시 세션 수의 제한	
안전한 경로/ 채널 (FTP)	FTP_ITC.1	안전한 채널	

[표 2] 도출된 SFR 목록

6.1.1. 보안감사(FAU)

6.1.2. 암호지원(FCS)

6.1.3. 사용자 데이터 보호(FDP)

6.1.4. 식별 및 인증(FIA)

6.1.5. 보안 관리(FMT)

6.1.6. TSF 보호(FPT)

6.1.7. TOE 접근(FTA)

6.2. 보증요구사항

본 보안목표명세서의 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 EAL4 이다. 다음 표는 CC Part 3에서 정의한 EAL4 보증 컴포넌트를 요약하여 보여준다.

보증클래스	CC Part3 보증 컴포넌트		국내용 평가보증등급
보안목표 명세서			
개발			
설명서			
생명주기지원			
시험			
취약성 평가			

[표 6] EAL4 보증패키지와 국내용 EAL4 평가보증등급

6.2. 보증요구사항

(가) ASE_INT.1 보안목표명세서 소개

종속관계	없음

개발자 요구사항

ASE_INT.1.1D	개발자는 보안목표명세서 소개를 제공해야 한다.

증거 요구사항

ASE_INT.1.1C	보안목표명세서 소개는 보안목표명세서 참조, TOE 참조, TOE 개요, TOE 설명을 포함해야 한다.
ASE_INT.1.2C	보안목표명세서 참조는 유일하게 보안목표명세서를 식별해야 한다.
ASE_INT.1.3C	TOE 참조는 TOE를 식별해야 한다.
ASE_INT.1.4C	TOE 개요는 TOE의 용도와 주요 보안 특성을 요약해야 한다.
ASE_INT.1.5C	TOE 개요는 TOE 유형을 식별해야 한다.
ASE_INT.1.6C	TOE 개요는 TOE에서 요구되는 비-TOE에 해당하는 하드웨어/소프트웨어/펌웨어를 식별해야 한다.
ASE_INT.1.7C	TOE 설명은 TOE의 물리적인 범위를 서술해야 한다.
ASE_INT.1.8C	TOE 설명은 TOE의 논리적인 범위를 서술해야 한다.

평가자 요구사항

ASE_INT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_INT.1.2E	평가자는 TOE 참조, TOE 개요, TOE 설명이 서로 일관성이 있음을 확인해야 한다.

(나) ASE_CCL.1 준수선언

종속관계	ASE_INT.1 보안목표명세서 소개 ASE_ECD.1 확장 컴포넌트 정의 ASE_REQ.1 명시된 보안요구사항

개발자 요구사항

ASE_CCL.1.1D	개발자는 준수 선언을 제공해야 한다.
ASE_CCL.1.2D	개발자는 준수 선언의 이론적 근거를 제공해야 한다.

증거 요구사항

ASE_CCL.1.1C	준수 선언은 보안목표명세서 및 TOE가 준수하는 공통평가기준의 버전을 식별하기 위해 공통평가기준 준수 선언을 포함해야 한다.
ASE_CCL.1.2C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 2부에 대한 준수 선언을 “2부 준수” 또는 “2부 확장”으로 서술해야 한다.
ASE_CCL.1.3C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 3부에 대한 준수 선언을 “3부 준수” 또는 “3부 확장”으로 서술해야 한다.
ASE_CCL.1.4C	공통평가기준 준수 선언은 확장 컴포넌트 정의와 일관성이 있어야 한다.
ASE_CCL.1.5C	준수 선언은 보안목표명세서가 준수하는 모든 보호프로파일 및 보안요구사항 패키지를 식별해야 한다.
ASE_CCL.1.6C	준수 선언은 보안목표명세서의 패키지에 대한 준수 선언을 '패키지 준수' 또는 '패키지 추가'로 서술해야 한다.
ASE_CCL.1.7C	준수 선언의 이론적 근거는 보안목표명세서의 TOE 유형이 그 보안목표명세서가 준수하는 보호프로파일의 TOE 유형과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.8C	준수 선언의 이론적 근거는 보안목표명세서의 보안문제정의에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안문제정의 설명과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.9C	준수 선언의 이론적 근거는 보안목표명세서의 보안목적에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안목적 설명과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.10C	준수 선언의 이론적 근거는 보안목표명세서의 보안요구사항에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안요구사항 설명과 일관성이 있음을 입증해야 한다.

평가자 요구사항

ASE_CCL.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ASE_SPD.1 보안문제정의

종속관계	없음

개발자 요구사항

ASE_SPD.1.1D	개발자는 보안문제정의를 제공해야 한다.

증거 요구사항

ASE_SPD.1.1C 보안문제정의는 위협을 서술해야 한다.

ASE_SPD.1.2C 모든 위협은 위협원, 자산, 악의적 행동의 관점에서 서술되어야 한다.

ASE_SPD.1.3C 보안문제정의는 조직의 보안정책(OSP)을 서술해야 한다.

ASE_SPD.1.4C 보안문제정의는 TOE 운영환경에 관한 가정사항을 서술해야 한다.

평가자 요구사항

ASE_SPD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ASE_OBJ.2 보안목적

종속관계 ASE_SPD.1 보안문제정의

개발자 요구사항

ASE_OBJ.1.1D 개발자는 보안목적에 대한 설명을 제공해야 한다.

증거 요구사항

ASE_OBJ.2.1C 보안목적에 대한 설명은 TOE 보안목적과 운영환경에 대한 보안목적을 서술해야 한다.

ASE_OBJ.2.2C 보안목적의 이론적 근거는 TOE에 대한 각 보안목적을 보안목적에 의해 대응되는 위협과 보안목적에 의해 수행되는 조직의 보안으로 추적해야 한다.

ASE_OBJ.2.3C 보안목적의 이론적 근거는 운영환경에 대한 각 보안목적을 보안목적에 의해 대응되는 위협, 보안목적에 의해 수행되는 조직의 보안정책, 보안목적에 의해 지원되는 가정사항으로 추적해야 한다.

ASE_OBJ.2.4C 보안목적의 이론적 근거는 보안목적이 모든 위협에 대응함을 입증해야 한다.

ASE_OBJ.2.5C 보안목적의 이론적 근거는 보안목적이 모든 조직의 보안정책을 수행함을 입증해야 한다.

ASE_OBJ.2.6C 보안목적의 이론적 근거는 운영환경에 대한 보안목적이 모든 가정사항을 지원함을 입증해야 한다.

평가자 요구사항

ASE_OBJ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(마) ASE_ECD.1 확장 컴포넌트 정의

종속관계	없음

개발자 요구사항

ASE_ECD.1.1D	개발자는 보안요구사항에 대한 설명을 제공해야 한다.
ASE_ECD.1.2D	개발자는 확장 컴포넌트 정의를 제공해야 한다.

증거 요구사항

ASE_ECD.1.1C	보안요구사항에 대한 설명은 확장된 모든 보안요구사항을 식별해야 한다.
ASE_ECD.1.2C	확장 컴포넌트 정의는 각각 확장된 보안요구사항에 대한 확장 컴포넌트를 정의해야 한다.
ASE_ECD.1.3C	확장 컴포넌트 정의는 각 확장 컴포넌트가 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 어떻게 연관되는지를 서술해야 한다.
ASE_ECD.1.4C	확장 컴포넌트 정의는 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 방법론을 모델로 하여 표현해야 한다.
ASE_ECD.1.5C	확장 컴포넌트는 각 엘리먼트에 대한 준수 여부를 입증할 수 있도록 측정 가능하고 객관적인 엘리먼트로 구성되어야 한다.

평가자 요구사항

ASE_ECD.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_ECD.1.2E	평가자는 확장된 컴포넌트가 기존의 컴포넌트를 이용하여 명확히 표현할 수 없음을 확인해야 한다.

(바) ASE_REQ.2 도출된 보안요구사항

종속관계	ASE_OBJ.2 보안목적 ASE_ECD.1 확장 컴포넌트 정의

개발자 요구사항

ASE_REQ.1.1D	개발자는 보안요구사항에 대한 설명을 제공해야 한다.
ASE_REQ.1.2D	개발자는 보안요구사항의 이론적 근거를 제공해야 한다.

증거 요구사항

ASE_REQ.2.1C 보안요구사항에 대한 설명은 보안기능요구사항과 보증요구사항을 서술해야 한다.

ASE_REQ.2.2C 보안기능요구사항 및 보증요구사항에서 사용되는 모든 주체, 객체, 오퍼레이션, 보안 속성, 외부 실체, 기타 용어들은 정의되어야 한다.

ASE_REQ.2.3C 보안요구사항에 대한 설명은 보안요구사항에 대한 모든 오퍼레이션을 식별해야 한다.

ASE_REQ.2.4C 모든 오퍼레이션은 정확히 수행되어야 한다.

ASE_REQ.2.5C 보안요구사항의 각 종속관계는 만족되어야 하며, 그렇지 않을 경우에는 보안요구사항의 이론적 근거에 그에 대한 정당화가 제공되어야 한다.

ASE_REQ.2.6C 보안요구사항의 이론적 근거는 각 보안기능요구사항을 TOE에 대한 보안목적으로 추적해야 한다.

ASE_REQ.2.7C 보안요구사항의 이론적 근거는 보안기능요구사항이 TOE에 대한 모든 보안목적을 만족한다는 것을 입증해야 한다.

보안요구사항의 이론적 근거는 보증요구사항이 선택된 이유를 설명해야 한다.

ASE_REQ.2.8C 보안요구사항에 대한 설명은 내부적으로 일관성이 있어야 한다.

평가자 요구사항

ASE_REQ.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(사) ASE_TSS.1 TOE 요약명세

종속관계 ASE_INT.1 보안목표명세서 소개
ASE_REQ.1 명시된 보안요구사항
ADV_FSP.1 기본적인 기능명세

개발자 요구사항

ASE_TSS.1.1D 개발자는 TOE 요약명세를 제공해야 한다.

증거 요구사항

ASE_TSS.1.1C TOE 요약명세는 TOE가 어떻게 각각의 보안기능요구사항을 만족시키는지 서술해야 한다.

평가자 요구사항

ASE_TSS.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ASE_TSS.1.2E 평가자는 TOE 요약명세가 TOE 개요 및 TOE 설명과 일관성이 있음을 확인해야 한다.

6.2.2. 개발

(가) ADV_ARC.1 기본적인 기능명세

종속관계 ADV_FSP.1 기본적인 기능명세
ADV_TDS.1 기본적인 설계

개발자 요구사항

ADV_ARC.1.1D 개발자는 TSF의 보안특성이 우회되지 않도록 TOE를 설계하고 구현해야 한다.

ADV_ARC.1.2D 개발자는 신뢰되지 않은 능동적 실체에 의한 침해로부터 TSF 자체를 보호할 수 있도록 TSF를 설계하고 구현해야 한다.

ADV_ARC.1.3D 개발자는 TSF의 보안 아키텍쳐 설명을 제공해야 한다.

증거 요구사항

ADV_ARC.1.1C 보안 아키텍쳐 설명은 TOE 설계문서에 서술된 SFR-수행 추상화 설명에 알맞은 상세 수준으로 서술되어야 한다.

ADV_ARC.1.2C 보안 아키텍쳐 설명은 TSF에 의해서 SFR과 일관성 있게 유지되어야 하는 보안영역을 서술해야 한다.

ADV_ARC.1.3C 보안 아키텍쳐 설명은 TSF 초기화 과정이 어떻게 안전한지 서술해야 한다.

ADV_ARC.1.4C 보안 아키텍쳐 설명은 TSF가 침해로부터 자신을 보호함을 입증해야 한다.

ADV_ARC.1.5C 보안 아키텍쳐 설명은 TSF가 SFR-수행 기능성의 우회를 방지함을 입증해야 한다.

평가자 요구사항

ADV_ARC.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ADV_FSP.4 완전한 기능명세

종속관계 없음

개발자 요구사항

ADV_FSP.4.1D 개발자는 기능명세를 제공해야 한다.

ADV_FSP.4.2D 개발자는 기능명세에서 SFR로의 추적성을 제공해야 한다.

증거 요구사항

ADV_FSP.4.1C	기능명세는 TSF를 완전하게 표현해야 한다.
ADV_FSP.4.2C	기능명세는 모든 TSFI에 대한 목적과 사용 방법을 서술해야 한다.
ADV_FSP.4.3C	기능명세는 각 TSFI와 관련된 모든 매개변수를 식별 및 서술해야 한다.
ADV_FSP.4.4C	기능명세는 각 TSFI에 관련된 모든 행동을 서술해야 한다.
ADV_FSP.4.5C	기능명세는 각 TSFI 호출 결과로 발생하는 모든 직접적인 오류메시지를 서술해야 한다.
ADV_FSP.4.6C	추적성은 SFR이 기능명세 내의 TSFI로 추적됨을 입증해야 한다.

평가자 요구사항

ADV_FSP.4.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ADV_FSP.4.2E	평가자는 기능명세가 SFR을 정확하고 완전하게 실체화하는지 결정해야 한다.

(다) ADV_IMP.1 TSF에 대한 구현의 표현

종속관계	ADV_TDS.3 기본적인 모듈화 설계 ALC_TAT.1 잘 정의된 개발 도구

개발자 요구사항

ADV_IMP.1.1D	개발자는 전체 TSF에 대한 구현의 표현을 가용하게 해야 한다.
ADV_IMP.1.2D	개발자는 TOE 설계 설명과 구현의 표현 표본간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_IMP.1.1C	구현의 표현은 더 이상의 설계과정 없이 TSF가 생성될 수 있는 상세수준으로 TSF를 정의해야 한다.
ADV_IMP.1.2C	구현의 표현은 개발 인력이 사용한 형태이어야 한다.
ADV_IMP.1.3C	TOE 설계 설명과 구현의 표현 표본간의 대응관계는 이들의 일치성을 입증해야 한다.

평가자 요구사항

ADV_IMP.1.1E	평가자는 선택된 구현의 표현 표본에 대해 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ADV_TDS.3 기본적인 모듈화 설계

종속관계 ADV_FSP.4 완전한 기능명세

개발자 요구사항

ADV_TDS.3.1D 개발자는 TOE 설계를 제공해야 한다.

ADV_TDS.3.2D 개발자는 기능명세의 TSFI와 TOE 설계에 사용 가능한 가장 상세수준 분해간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_TDS.3.1C 설계는 TOE의 구조를 서브시스템 측면에서 서술해야 한다.

ADV_TDS.3.2C 설계는 TSF를 모듈 측면에서 서술해야 한다.

ADV_TDS.3.3C 설계는 TSF의 모든 서브시스템을 식별해야 한다.

ADV_TDS.3.4C 설계는 TSF의 각 서브시스템에 대한 설명을 제공해야 한다.

ADV_TDS.3.5C 설계는 TSF의 모든 서브시스템들 간의 상호작용에 대한 설명을 제공해야 한다.

ADV_TDS.3.6C 설계는 TSF 서브시스템과 TSF 모듈간의 대응관계를 제공해야 한다.

ADV_TDS.3.7C 설계는 각 SFR-수행 모듈을 그 목적 및 다른 모듈 간의 상관관계 측면에서 서술해야 한다.

ADV_TDS.3.8C 설계는 각 SFR-수행 모듈을 SFR-관련 인터페이스, 인터페이스로부터의 반환 값, 다른 모듈과의 상호작용 및 다른 SFR-수행 모듈에서 호출된 SFR-관련 인터페이스 측면에서 서술해야 한다.

ADV_TDS.3.9C 설계는 각 SFR-지원 또는 SFR-비-간섭 모듈을 목적 및 다른 모듈과의 상호작용 측면에서 서술해야 한다.

ADV_TDS.3.10C 대응관계는 모든 TSFI가 자신이 호출하는 TOE 설계 내에 서술된 행동으로 추적됨을 입증해야 한다.

평가자 요구사항

ADV_TDS.31E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ADV_TDS.32E 평가자는 설계가 모든 보안기능요구사항을 정확하고 완전하게 실체화하는지 결정해야 한다.

6.2.3. 설명서

(가) AGD_OPE.1 사용자 운영 설명서

종속관계 ADV_FSP.1 기본적인 기능명세

개발자 요구사항

AGD_OPE.1.1D 개발자는 사용자 운영 설명서를 제공해야 한다.

증거 요구사항

AGD_OPE.1.1C 사용자 운영 설명서는 각각의 사용자 역할에 대해 안전한 처리환경 내에서 통제되어야 하는 사용자가 접근 가능한 기능 및 특권에 대해 적절한 경고를 포함해서 서술해야 한다.

AGD_OPE.1.2C 사용자 운영 설명서는 각각의 사용자 역할에 대해 TOE에 의해 안전한 방식으로 제공되는 인터페이스의 사용 방법을 서술해야 한다.

AGD_OPE.1.3C 사용자 운영 설명서는 각각의 사용자 역할에 대해 사용 가능한 기능 및 인터페이스를 서술해야 한다. 특히 사용자의 통제 하에 있는 모든 보안 매개변수에 대해 안전한 값을 적절하게 표시해야 한다.

AGD_OPE.1.4C 사용자 운영 설명서는 각각의 사용자 역할에 대해, 수행되어야 할 사용자가 접근할 수 있는 기능과 연관된 보안-관련 사건의 각 유형을 명확히 제시해야 한다. 여기에는 TSF의 통제 하에 있는 실체에 대한 보안 특성의 변경도 포함되어야 한다.

AGD_OPE.1.5C 사용자 운영 설명서는 (장애 후의 운영 또는 운영상의 오류 후의 운영을 포함한) TOE의 모든 가능한 운영 모드, 그 영향 및 안전한 운영 유지를 위한 관련사항들을 식별해야 한다.

AGD_OPE.1.6C 사용자 운영 설명서는 각각의 사용자 역할에 대해 보안목표명세서에 기술된 대로 운영환경에 대한 보안목적을 만족시키기 위해 준수해야 하는 보안대책을 서술해야 한다

AGD_OPE.1.7C 사용자 운영 설명서는 명확하고 타당해야 한다.

평가자 요구사항

AGD_OPE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) AGD_PRE.1 준비 절차

종속관계 없음

개발자 요구사항

AGD_PRE.1.1D 개발자는 준비 절차를 포함하여 TOE를 제공해야 한다.

증거 요구사항

AGD_PRE1.1C 준비 절차는 배포된 TOE의 안전한 인수를 위해 필요한 모든 단계를 개발자의 배포 절차와 일관되게 서술해야 한다.

AGD_PRE1.2C 준비 절차는 TOE의 안전한 설치 및 운영환경의 안전한 준비를 위해 필요한 모든 단계를 보안목표명세서에 기술된 운영환경에 대한 보안목적과 일관되게 서술해야 한다.

평가자 요구사항

AGD_PRE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

AGD_PRE.1.2E 평가자는 TOE가 운영을 위해 안전하게 준비될 수 있음을 확인하기 위해 준비 절차를 적용해야 한다.

6.2.4. 생명주기 지원

(가) ALC_CMC.4 생산지원, 수용절차 및 자동화

종속관계 ALC_CMS.1 TOE 형상관리 범위
ALC_DVS.1 보안대책의 식별
ALC_LCD.1 개발자가 정의한 생명주기 모델

개발자 요구사항

ALC_CMC.4.1D 개발자는 TOE 및 그에 대한 참조를 제공해야 한다.

ALC_CMC.4.2D 개발자는 형상관리 문서를 제공해야 한다.

ALC_CMC.4.3D 개발자는 형상관리 시스템을 사용해야 한다.

증거 요구사항

ALC_CMC.4.1C TOE는 유일한 참조를 위한 레이블을 붙여야 한다.

ALC_CMC.4.2C 형상관리 문서는 형상항목을 유일하게 식별하는 데 사용된 방법을 서술해야 한다.

ALC_CMC.4.3C 형상관리 시스템은 모든 형상항목을 유일하게 식별해야 한다.

ALC_CMC.4.4C 형상관리 시스템은 형상항목에 인가된 변경만을 허용하는 자동화된 수단을 제공해야 한다.

ALC_CMC.4.5C 형상관리 시스템은 자동화된 수단을 이용하여 TOE의 생산을 지원해야 한다.

ALC_CMC.4.6C 형상관리 문서는 형상관리 계획을 포함해야 한다.

ALC_CMC.4.7C 형상관리 계획은 형상관리 시스템이 TOE 개발에 사용되는 방법을 서술해야 한다.

ALC_CMC.4.8C 형상관리 계획은 변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는데 사용된 절차를 서술해야 한다.

ALC_CMC.4.9C 증거는 모든 형상항목이 형상관리 시스템 하에 유지되고 있음을 입증해야 한다.

ALC_CMC.4.10C 증거는 형상관리 시스템이 형상관리 계획에 따라 운영되고 있음을 입증해야 한다.

평가자 요구사항

ALC_CMC.4.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ALC_CMS.4 문제추적 형상관리 범위

종속관계 없음

개발자 요구사항

ALC_CMS.4.1D 개발자는 TOE에 대한 형상목록을 제공해야 한다.

증거 요구사항

ALC_CMS.4.1C 형상목록은 TOE, 보증요구사항에서 요구하는 평가증거, TOE를 구성하는 부분, 구현 표현, 보안 결함 보고서 및 해결 상태를 포함해야 한다.

ALC_CMS.4.2C 형상목록은 형상항목을 유일하게 식별해야 한다.

ALC_CMS.4.3C 형상목록은 각 TSF 관련 형상항목의 개발자를 표시해야 한다.

평가자 요구사항

ALC_CMS.4.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ALC_DEL.1 배포 절차

종속관계 없음

개발자 요구사항

ALC_DEL.1.1D 개발자는 소비자에게 TOE나 TOE 일부를 배포하는 절차를 문서화하여 제공해야 한다.

ALC_DEL.1.2D 개발자는 배포 절차를 사용해야 한다.

증거 요구사항

ALC_DEL.1.1C	배포 문서는 TOE를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 절차를 서술해야 한다.

평가자 요구사항

ALC_DEL.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ALC_DVS.1 보안대책의 식별

종속관계	없음

개발자 요구사항

ALC_DVS.1.1D	개발자는 개발보안 문서를 작성하여 제공해야 한다.

증거 요구사항

ALC_DVS.1.1C	개발보안 문서는 개발환경 내에서 TOE 설계 및 구현 과정의 비밀성과 무결성을 보호하기 위하여 필요한 물리적, 절차적, 기술적 및 기타 보안대책을 서술해야 한다.

평가자 요구사항

ALC_DVS.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ALC_DVS.1.2E	평가자는 보안대책이 적용되고 있는지 확인해야 한다.

(마) ALC_LCD.1 개발자가 정의한 생명주기 모델

종속관계	없음

개발자 요구사항

ALC_LCD.1.1D	개발자는 TOE의 개발과 유지에 사용되는 생명주기 모델을 수립해야 한다.
ALC_LCD.1.2D	개발자는 생명주기 정의 문서를 제공해야 한다.

증거 요구사항

ALC_LCD.1.1C	생명주기 정의 문서는 TOE의 개발과 유지에 사용되는 모델을 서술해야 한다.
ALC_LCD.1.2C	생명주기 모델은 TOE의 개발과 유지에 필요한 통제를 제공해야 한다.

평가자 요구사항

ALC_LCD.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(바) ALC_TAT.1 잘 정의된 개발 도구

종속관계	ADV_IMP.1 TSF에 대한 구현의 표현

개발자 요구사항

ALC_TAT.1.1D	개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.
ALC_TAT.1.2D	개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.

증거 요구사항

ALC_TAT.1.1C	구현에 사용된 각 개발 도구는 잘 정의된 것이어야 한다.
ALC_TAT.1.2C	각 개발 도구 문서는 구현에 사용된 모든 규정과 지시어 뿐만 아니라 모든 명령문의 의미를 모호하지 않게 정의해야 한다.
ALC_TAT.1.3C	각 개발 도구 문서는 모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의해야 한다.

평가자 요구사항

ALC_TAT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

6.2.5. 시험

(가) ATE_COV.2 시험범위의 분석

종속관계	ADV_FSP.2 보안-수행 기능명세 ATE_FUN.1 기능 시험

개발자 요구사항

ATE_COV.2.1D	개발자는 시험범위의 분석을 제공해야 한다.

증거 요구사항

ATE_COV.2.1C	시험범위의 분석은 시험 문서 내의 시험항목과 기능명세 내의 TSFI간의 일치성을 입증해야 한다.
ATE_COV.2.2C	시험범위의 분석은 기능명세 내의 모든 TSFI가 시험되었음을 입증해야 한다.

평가자 요구사항

ATE_COV.2.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ATE_DPT.1 기본설계 시험

종속관계 ADV_ARC.1 보안 아키텍쳐 설명
ADV_TDS.2 아키텍쳐 설계
ATE_FUN.1 기능 시험

개발자 요구사항

ATE_DPT.1.1D 개발자는 시험의 상세수준 분석을 제공해야 한다.

증거 요구사항

ATE_DPT.1.1C 시험의 상세수준 분석은 시험 문서 내의 시험항목과 TOE 설계 내의 TSF 서브시스템 간의 일치성을 입증해야 한다.

ATE_DPT.1.2C 시험의 상세수준 분석은 TOE 설계 내의 모든 TSF 서브시스템이 시험되었음을 입증해야 한다.

평가자 요구사항

ATE_DPT.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ATE_FUN.1 기능 시험

종속관계 ATE_COV.1 시험범위의 증거

개발자 요구사항

ATE_FUN.1.1D 개발자는 TSF를 시험하고 그 결과를 문서화해야 한다.

ATE_FUN.1.2D 개발자는 시험 문서를 제공해야 한다.

증거 요구사항

ATE_FUN.1.1C 시험 문서는 시험계획, 예상 시험결과, 실제 시험결과로 구성되어야 한다.

ATE_FUN.1.2C 시험계획은 수행되어야 할 시험항목을 식별하고 각 시험 수행의 시나리오를 서술해야 한다. 이러한 시나리오는 다른 시험결과에 대한 순서 종속관계를 포함해야 한다.

ATE_FUN.1.3C 예상 시험결과는 시험의 성공적인 수행으로 기대되는 결과를 제시해야 한다.

ATE_FUN.1.4C 실제 시험결과는 예상 시험결과와 일관성이 있어야 한다.

평가자 요구사항

ATE_FUN.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ATE_IND.2 독립적인 시험 : 표본 시험

종속관계
- ADV_FSP.2 보안-수행 기능명세 기능명세
- AGD_OPE.1 사용자 운영 설명서
- AGD_PRE.1 준비 절차
- ATE_COV.1 시험범위의 증거
- ATE_FUN.1 기능 시험

개발자 요구사항

ATE_IND.2.1D 개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항

ATE_IND.2.1C TOE는 시험하기에 적합해야 한다.

ATE_IND.2.2C 개발자는 개발자의 TSF 기능 시험에 사용된 자원과 동등한 자원을 제공해야 한다.

평가자 요구사항

ATE_IND.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ATE_IND.2.2E 평가자는 개발자 시험 결과를 검증하기 위하여 시험문서 내의 시험항목에 대한 표본 시험을 수행해야 한다.

ATE_IND.2.3E 평가자는 TSF가 명세된대로 동작함을 확인하기 위하여 TSF의 일부를 시험해야 한다.

6.2.6. 취약성 평가

(가) AVA_VAN.3 집중화된 취약성 분석

종속관계
- ADV_ARC.1 보안 아키텍쳐 설명
- ADV_FSP.4 완전한 기능명세
- ADV_TDS.3 기본적인 모듈화 설계
- ADV_IMP.1 TSF에 대한 구현의 표현
- AGD_OPE.1 사용자 운영 설명서
- AGD_PRE.1 준비 절차
- ATE_DPT.1 기본설계 시험

개발자 요구사항

AVA_VAN.3.1D 개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항

AVA_VAN.3.1C TOE는 시험하기에 적합해야 한다.

평가자 요구사항

AVA_VAN.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

AVA_VAN.3.2E 평가자는 TOE의 잠재적 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다.

AVA_VAN.3.3E 평가자는 TOE의 잠재적 취약성을 식별하기 위해 설명서, 기능명세, TOE 설계 및 보안 아키텍쳐 설명, 구현의 표현을 이용하여 집중화된 독립적인 취약성 분석을 수행해야 한다.

AVA_VAN.3.4E 평가자는 TOE가 강화된-기본 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 결정하기 위해, 식별된 잠재적 취약성에 근거하여 침투시험을 수행해야 한다.

6.3. 보안요구사항의 이론적 근거

6.3.1. 보안기능요구사항의 이론적 근거

보안기능요구사항의 이론적 근거는 다음을 입증한다.

▷ 각 TOE 보안목적은 적어도 하나의 TOE 보안기능요구사항에 의해 다루어진다.

▷ 각 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다.

보안기능 요구사항	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.

[보안목적과 보안기능요구사항 대응]

O.	컴포넌트1, 컴포넌트2,
O.	컴포넌트1, 컴포넌트2,

6.3.2. 보증요구사항의 이론적 근거

☞ 평가보증등급을 선택한 이유를 서술

☞ 평가보증 패키지에서 ST 작성자가 보증컴포넌트를 추가한 경우 추가한 이유를 서술

6.4. 종속관계에 대한 이론적 근거

6.4.1. 보안기능요구사항의 종속관계

다음 표는 보안기능요구사항의 종속관계를 보여준다.

번호	ST 보안기능요구사항	CC 제2부 보안기능요구사항 종속관계	본 표에서 SFR 식별을 위해 부여한 번호

[표 7] 종속관계 이론적 근거

☞ 종속관계를 만족하지 못하는 경우 정당성 근거를 제시

6.4.2. 보증요구사항의 종속관계

정보보호시스템 공통평가기준에서 제공하는 EAL4 보증 패키지의 종속관계는 이미 만족되어 있으므로 이에 대한 이론적 근거는 생략한다.

07

TOE 요약명세

7. TOE 요약명세

7.1. TOE 보안기능성

☞ 보안기능요구사항을 만족시키기 위해 TOE에서 구현한 메커니즘, 기능 등을 설명

7.1.1. 사용자 데이터보호

7.1.2. TOE 접근

7.1.3. 식별 및 인증

7.1.4. 안전한 경로/채널

7.1.5. 보안감사

7.1.6. 보안관리

7.1.7. TSF 보호

7.1.8. 암호지원

08

참고자료

8. 참고자료

자료 명	저 자	비 고
정보보호시스템 공통평가기준 버전 3.1 개정 2판 •정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1R1, 2006. 9., CCMB-2006-09-001 •정보보호시스템 공통평가기준 2부 : 보안기능요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-002 •정보보호시스템 공통평가기준 3부 : 보증요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-003	CCRA	2007. 9

09

용어 및 약어

9. 용어 및 약어

CC	Common Criteria
CCMB	Common Criteria Maintenance Board
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IT	Information Technology
NTP	Network Time Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network
SSH	Secure Shell
TLS	Transport Layer Security