국가보안기술연구소

정보보호제품 평가·인증제도 및 국제상호인정협정(CCRA) 동향

2022. 6. 10.

IT보안인증사무국

CONTENTS

01

정보보호제품 평가•인증제도 현황

'정보보증': '정보보호가 얼마나 잘 이루어지고 있는가?'에 대한 신뢰를 의미
'신뢰의 수준' ☞ '정보보증의 수준'

필요성(Needs)

- ICT 환경이 안전한가?
- ICT 제품을 신뢰할 수 있는가?

평가(Evaluation)

- 제3자가 평가방법론 사용하여 IT제품이 평가기준에 부합하는지 확인

인증(Certification)

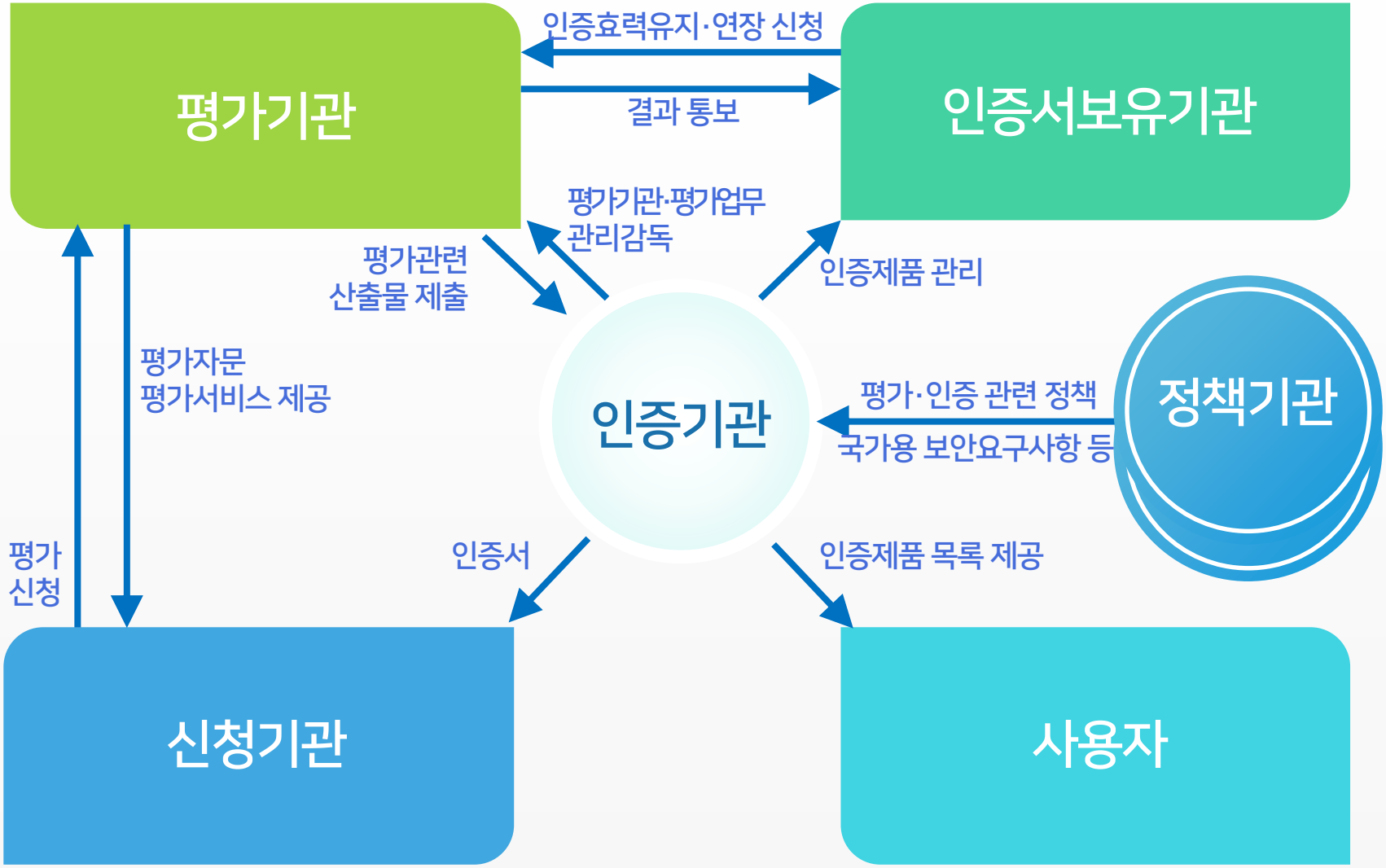
- 공신력 있는 기관이 평가 과정에서 평가기준 및 평가방법론을 정확하게 적용했는지 감독

관계 법령•행정규칙•규정

법령	지능정보화 기본법 제58조	(정보보호시스템에 관한 기준 고시 등)
	지능정보화 기본법 시행령 제51조	(정보보호시스템에 관한 기준 고시 등)
행정규칙	정보보호시스템 평가•인증 지침	공통평가기준(CC)를 적용한 평가•인증 체계 고시
	정보보호시스템 공통평가기준	공통평가기준(CC) 고시
세부절차	정보보호제품 평가•인증 수행규정	국제상호인정협정(CCRA)에 따른 CC평가•인증 규정
	정보보호제품 국내용 평가•인증 세부 수행절차	국가•공공기관 도입 목적의 국내용 CC평가•인증 규정

개발•평가•인증•사용 관계도

정보보호제품 평가•인증체계



CC인증제도 연혁 (1)

1995

(8월) 정보보호제품 평가•인증 근거 법령 제정 (정보화촉진기본법→국가정보화기본법→現지능정보화기본법)

1998

(2월) K등급제도 침입차단시스템 평가기준 제정 및 평가•인증 시행

2000

(2월) K등급제도 침입탐지시스템 평가기준 제정 및 평가•인증 시행

2002

(8월) 정보보호시스템 공통평가기준(CC V2.1) 도입 및 적용 (CC/K기준 평가•인증 이원화)

2005

(5월) 정보보호시스템 공통평가기준(CC V2.3)으로 평가기준 단일화
(11월) 국제상호인정협정(CCRA) 인증서발행국 가입 심사

2006

(5월) 국제상호인정협정(CCRA) 인증서발행국 가입 승인

CC인증제도 연혁 (2)

2007
(4월) 국내용 평가•인증제도 도입 (국제용 제도와 국내용 제도로 이원화)

2008
(4월) 공통평가기준 개정 적용 (CC V2.3→CC V3.1)
(9월) 국제상호인정협정(CCRA) 정기회의 및 ICCC 2009 개최

2010
(4월) 국내용 평가•인증제도 개선

2012
(11월) 정책기관(국가정보원) 및 인증기관(국가보안기술연구소) 구분
(11월) 국제상호인정협정(CCRA) 인증서발행국 정기심사

2014
(7월~9월) CCRA 협정서 개정안 확정 및 전체 회원국 서명
(10월) 정책기관 변경 (국가정보원→미래창조과학부)

2016
(4월) 국제상호인정협정(CCRA) 정기회의 개최

CC인증제도 연혁 (3)

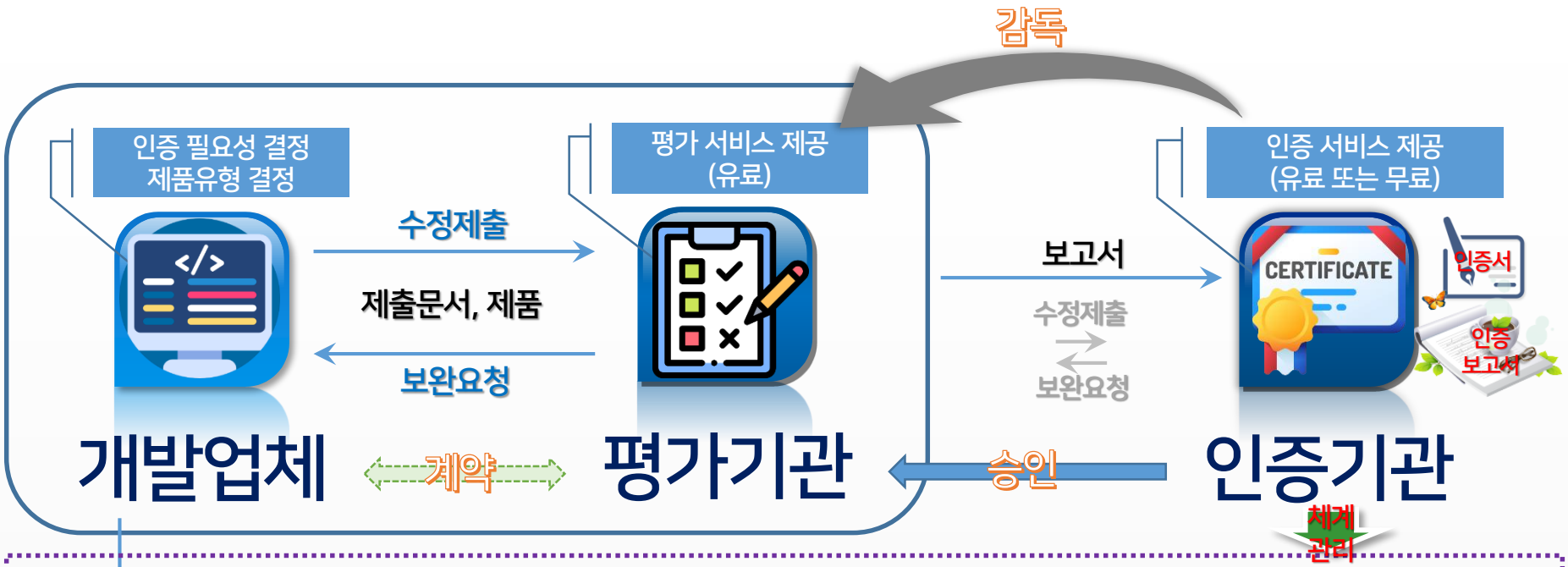
2017

(6월) 정보보호제품 평가•인증 수행규정 개정 (CCRA 인증서발행국 정기심사 대비)
(9월) 정보보호제품 평가•인증 수행규정 개정 (미래창조과학부 → 現과학기술정보통신부)
(10월~11월) 국제상호인정협정(CCRA) 인증서발행국 정기심사

2021

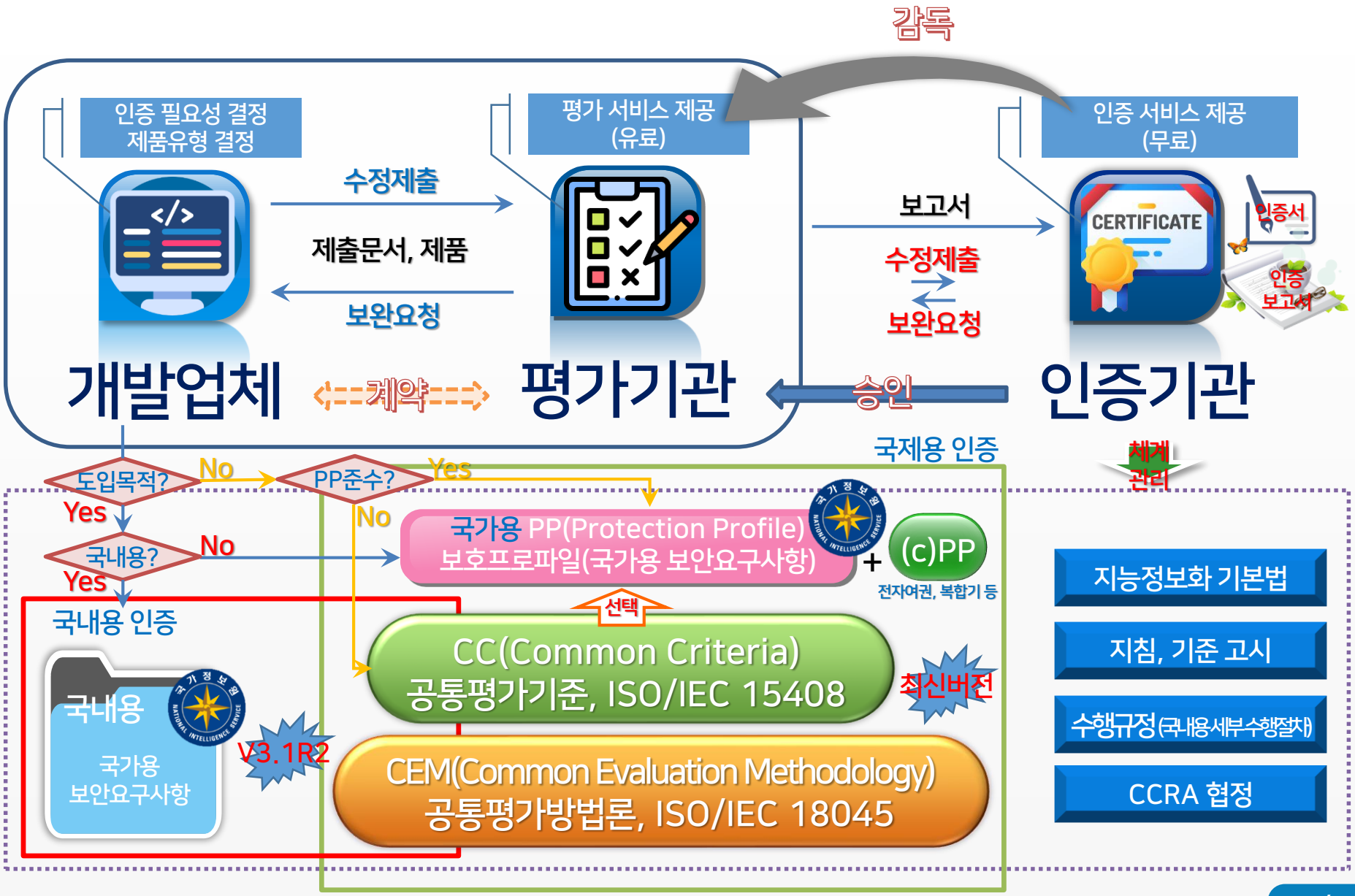
(5월) 정보보호제품 평가•인증 수행규정 개정 (정보보호제품 국내용 평가•인증 세부 수행절차 개정)

CCRA 협정에 따른 CC 평가•인증 개요



- 법령
- 행정령
- 관련 규정
- CCRA 협정

국내의 CC 평가•인증 개요 (국제용 & 국내용)



CC 인증서 및 트레이드 마크

인 증 서

KECS-0000-0000-0000

제품명

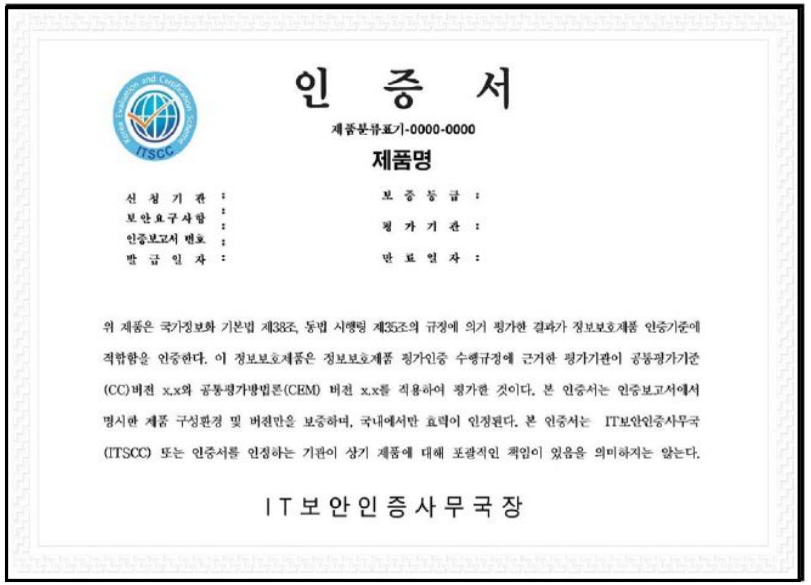
신 청 기 관 :	보호프로파일 :
제 품 유 형 :	평 가 기 관 :
제 품 버 전 :	발 급 일 자 :
인증보고서 번호 :	만 료 일 자 :
평가보증등급 :	

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증합니다.

이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC) [버전]과 공통평가방법론(CEM) [버전]을 적용하여 평가한 것이다. 본 인증서는 인증보고서에서 명시한 제품 구성환경 및 해당 버전만을 보증한다. 평가는 정보보호제품 평가인증 수행규정에서 정한 절차에 따라 수행되었으며, 평가결과보고서의 내용은 평가세부결과와 일치한다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

국제용 인증서 (한글, 영어)



인 증 서

제품분류표기-0000-0000

제품명

신 청 기 관 :	보 증 등 급 :
보안요구사항 :	
인증보고서 번호 :	평 가 기 관 :
발 급 일 자 :	만 료 일 자 :

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증한다. 이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC)버전 x.x와 공통평가방법론(CEM) 버전 x.x를 적용하여 평가한 것이다. 본 인증서는 인증보고서에서 명시한 제품 구성환경 및 버전만을 보증하며, 국내에서만 효력이 인정된다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

국내용 인증서 (한글)

국가보안기술연구소 트레이드 마크

CCRA CC인증

CCRA 상호인정 서비스

IT보안인증사무국

02

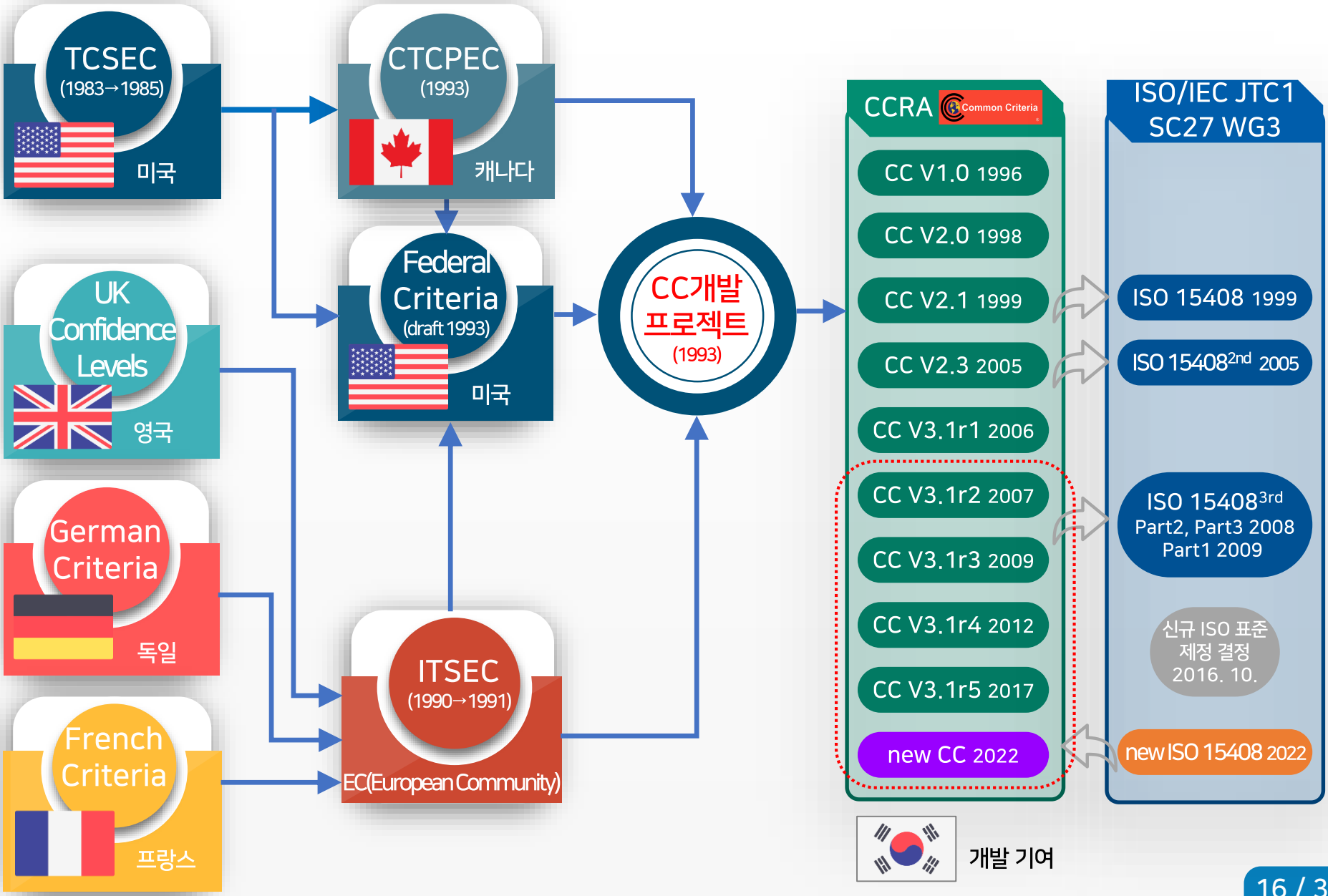
CC/CEM 동향

CC의 개발 배경 및 필요성

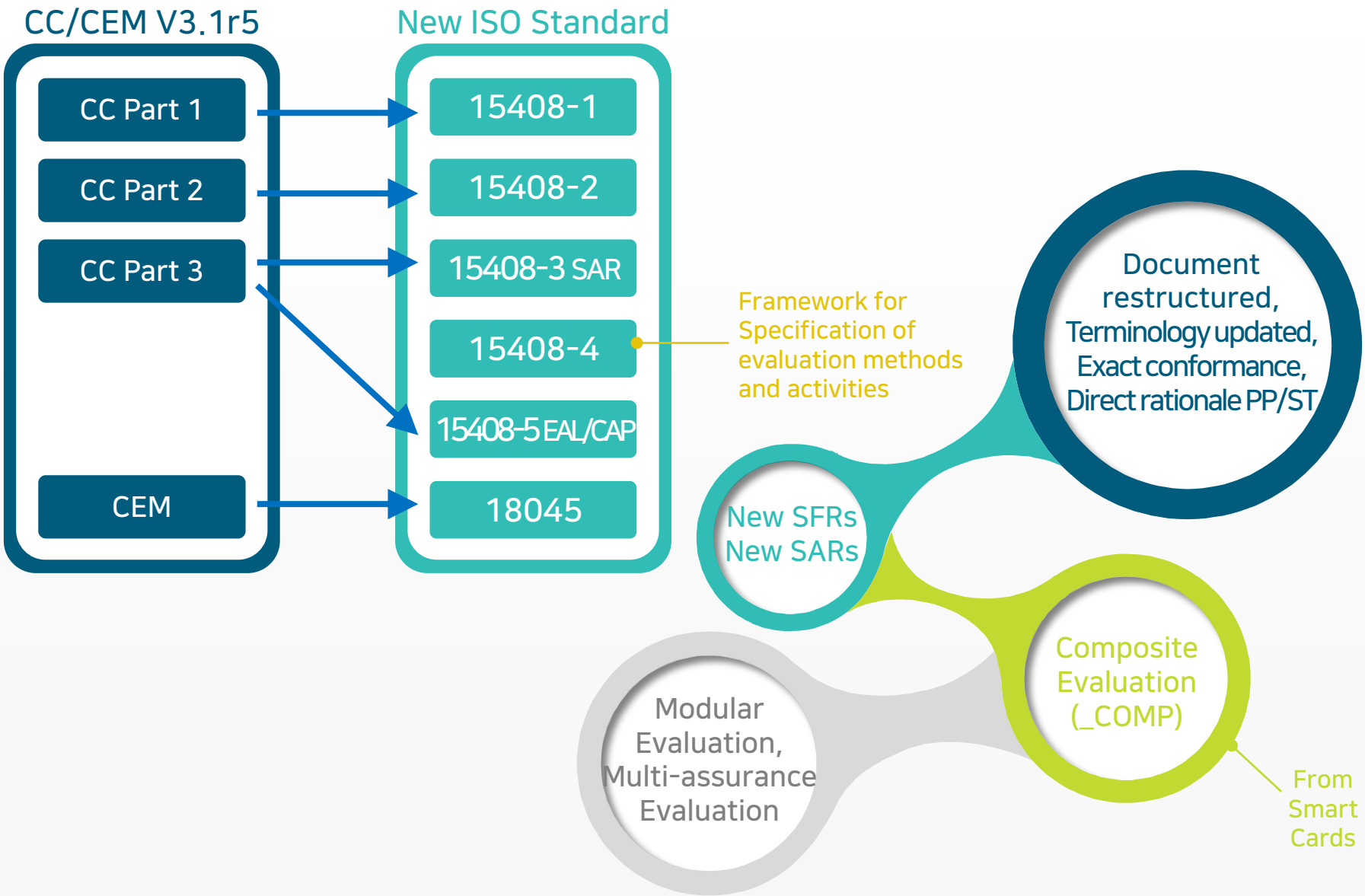
Common Criteria®

IT 보안을 표현하기 위해 국제적으로 동의한 체계
ISO/IEC 표준과 연계하여 개발
보안기능과 보증요구사항의 표준 분류를 제공

CC 연혁


TCSEC
(1983→1985)
미국
CTCPEC
(1993)
캐나다
Federal
Criteria
(draft 1993)
미국
UK
Confidence
Levels
영국
German
Criteria
독일
French
Criteria
프랑스
ITSEC
(1990→1991)
EC(European Community)
CC개발
프로젝트
(1993)
CCRA
Common Criteria
CC V1.0 1996
CC V2.0 1998
CC V2.1 1999
CC V2.3 2005
CC V3.1r1 2006
CC V3.1r2 2007
CC V3.1r3 2009
CC V3.1r4 2012
CC V3.1r5 2017
new CC 2022
ISO/IEC JTC1
SC27 WG3
ISO 15408 1999
ISO 15408 2nd 2005
ISO 15408 3rd
Part2, Part3 2008
Part1 2009
신규 ISO 표준
제정 결정
2016. 10.
new ISO 15408 2022
개발 기여

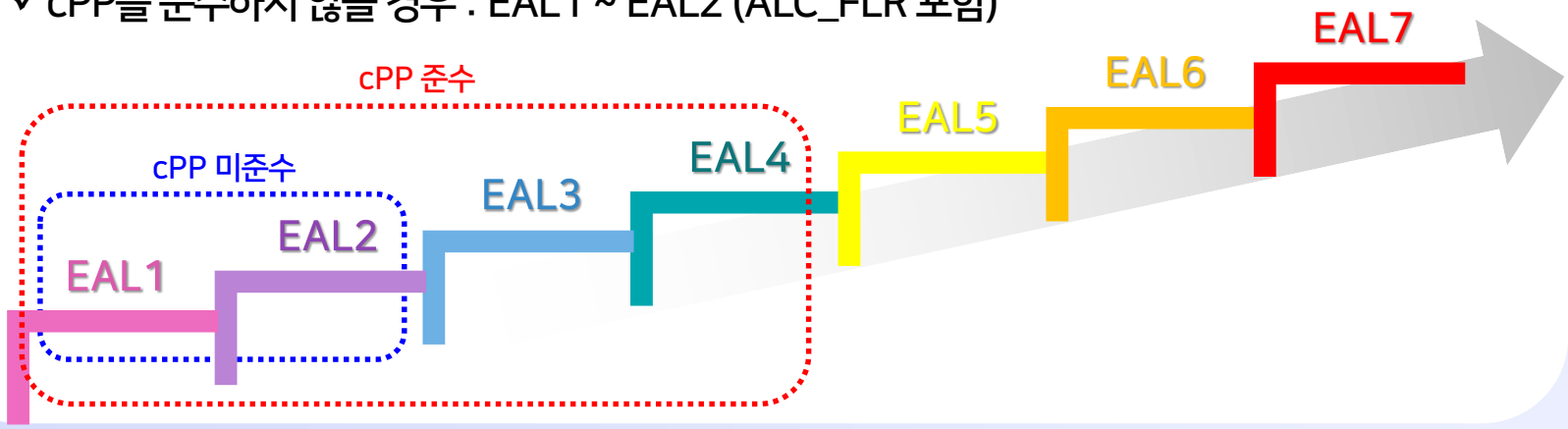
CC/CEM 주요 개정사항



03

국제상호인정협정(CCRA) 동향

- **국제상호인증협정(CCRA)** : CC를 적용하여 평가•인증한 결과 발급된 인증서를 회원국간에 상호인정하기 위한 협정 (2000년 발족)
  - ✓인증서는 인증서발행국의 인증기관에서 발급 가능
  - ✓CCRA : Common Criteria Recognition Arrangement
  - ✓www.commoncriteriaportal.org
- **상호인정 범위** (2014년도 협정서 개정)
  - ✓cPP를 준수할 경우 : EAL1 ~ EAL4 (ALC_FLR 포함) (EAL2 이하 포함 권고)
  - ✓cPP를 준수하지 않을 경우 : EAL1 ~ EAL2 (ALC_FLR 포함)



국제상호인정협정(CCRA) 주요 변경사항

NSR

주요 내용	개정 前 (2000.5월)	개정 後 (2014.7월)
상호인정 범위	EAL1 ~ EAL4 CC 인증서	cPP 준수 CC 인증서 (최대 EAL4까지 포함 가능) 또는 EAL1 ~ EAL2 CC 인증서
상호인정 거부	자국의 법률, 관계 법령, 행정 규제, 공적 의무 등에 의해 거절 가능	자국의 법률, 관계 법령, 행정 규제, 등에 의해 거절 가능 규정 제공 강력히 권고
상호인정 기반 기술문서	CC (공통평가기준) CEM (공통평가방법론)	CC (공통평가기준) CEM (공통평가방법론) 보조문서

비용효율성
일관성
반복가능성

※ cPP (collaborative Protection Profile, 공동 보호프로파일)
: CCRA에서 승인한 iTC(international Technical Community)에서 개발

Certificate Validity: 인증서 관리적 유효기간을 5년 이내로 정하고 재평가를 통해 연장되지 않는 제품은 만료 처리('19.6.1. 시행)

국제상호인정협정(CCRA) 회원국 변동사항

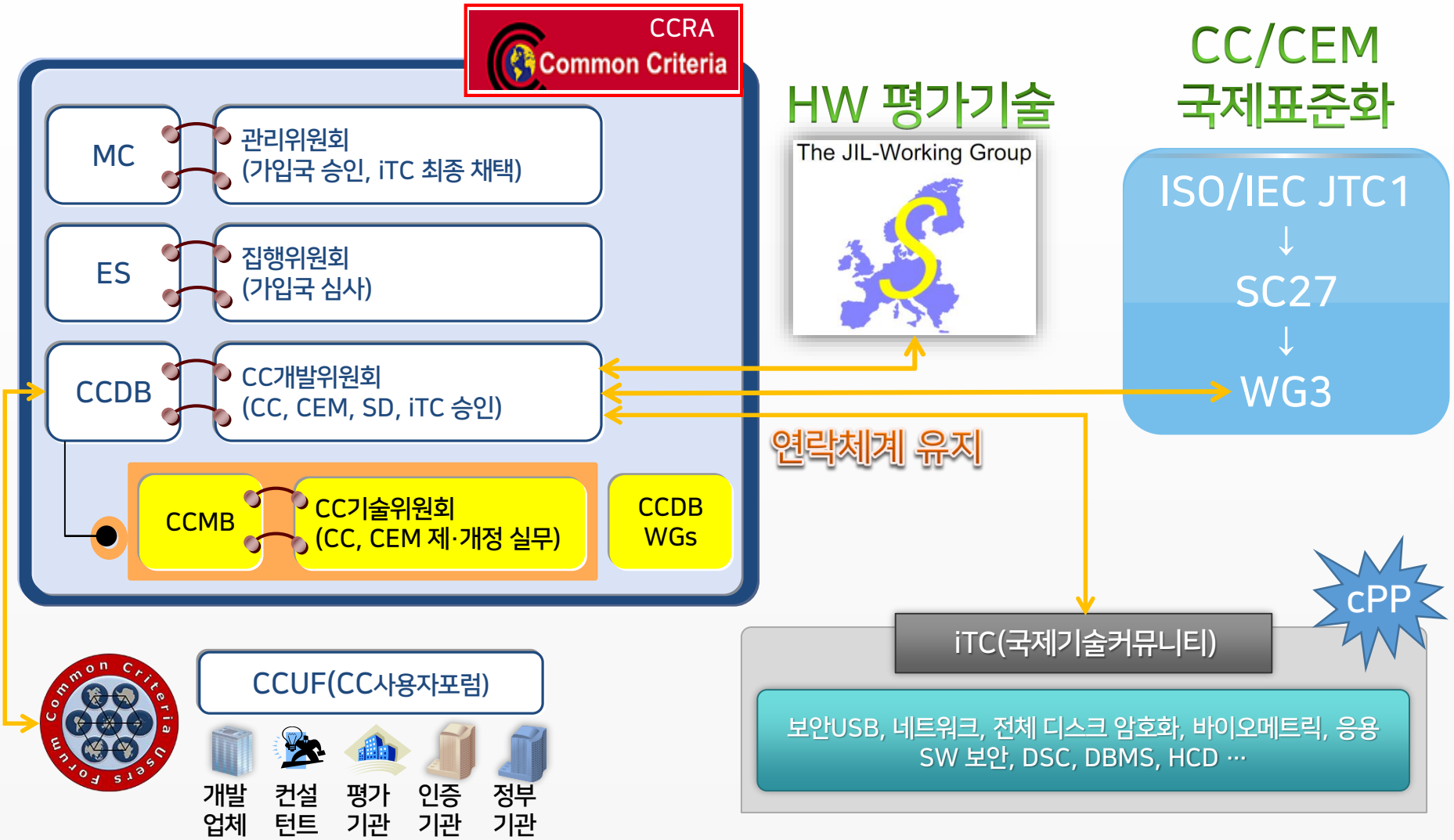
인증서 발행국 (16개국)

인증서 수용국 (15개국)

- 영국 : 인증서발행국 → 인증서수용국 (2019)
- 뉴질랜드 : 인증서발행국 → 인증서수용국 (2021)

자발적 전환

국제상호인정협정(CCRA) 위원회 및 국제협력 기구

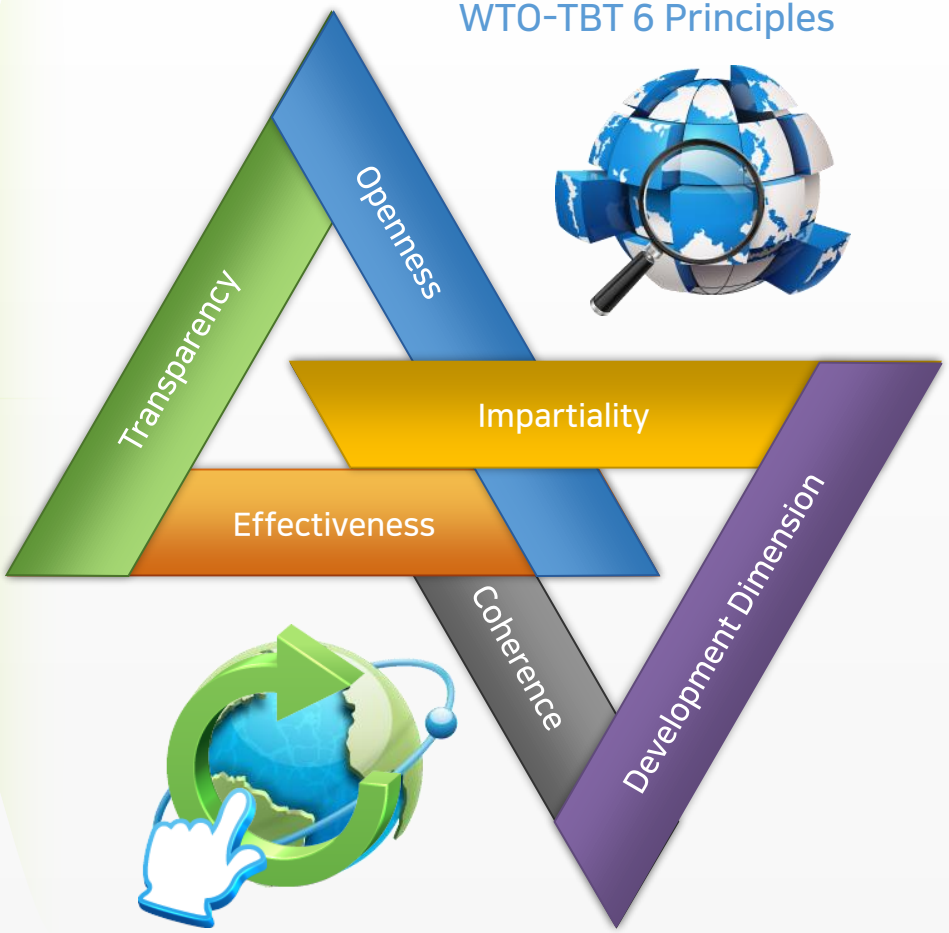


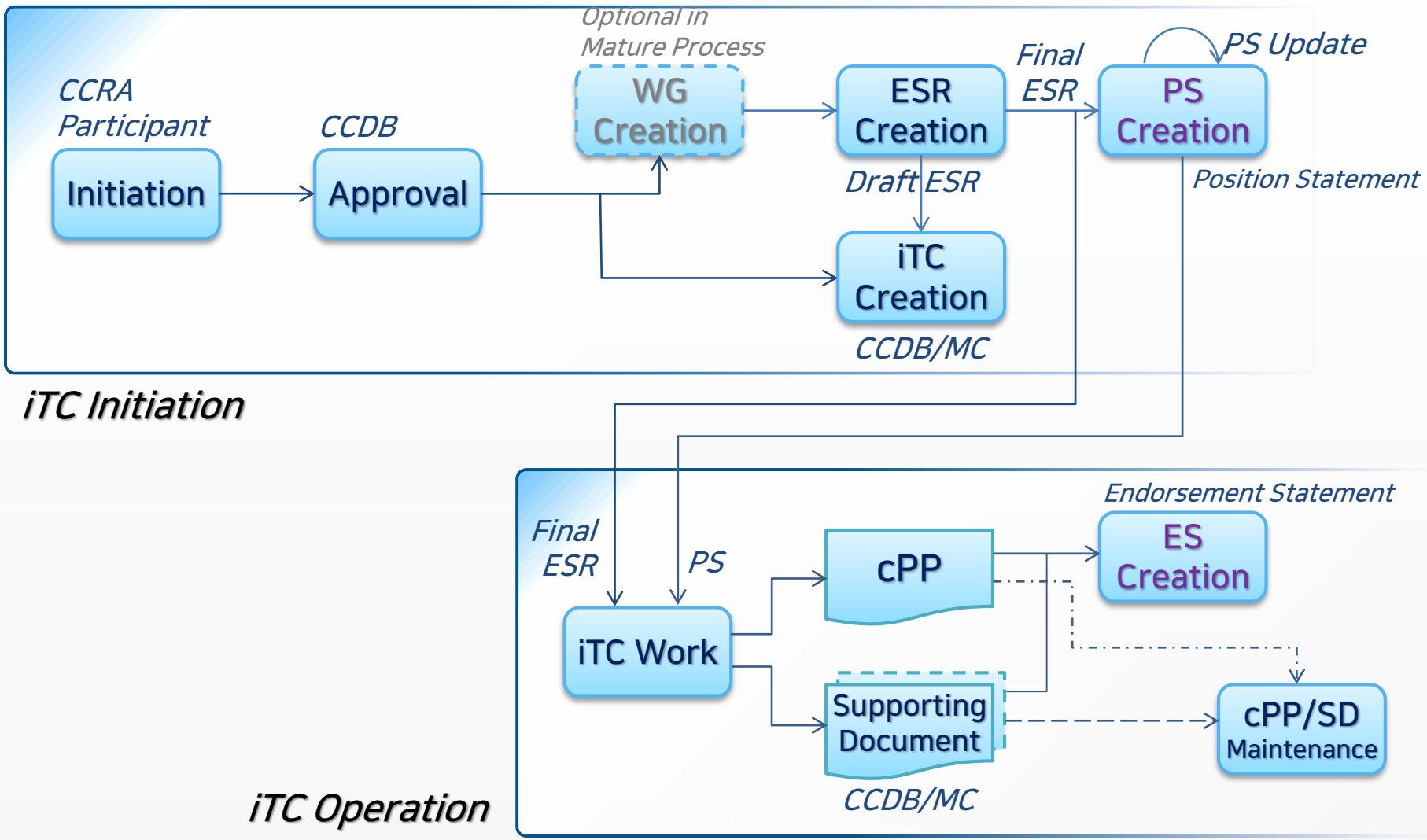
cPP 기반 상호인정 모델

Endorsed iTCs

- Application Software
- Biometrics Security
- Database Management Systems
- Dedicated Security Components
- Full Disk Encryption
- Hardcopy Devices
- Network Fundamentals and Firewall
- USB Portable Storage Devices

"Establishing iTCs and Developing cPPs "




Optional in
Mature Process
CCRA
Participant
CCDB
Initiation
Approval
WG
Creation
ESR
Creation
Final
ESR
PS Update
PS
Creation
Draft ESR
Position Statement
iTC
Creation
CCDB/MC
iTC Initiation
Endorsement Statement
Final
ESR
PS
cPP
ES
Creation
iTC Work
Supporting
Document
cPP/SD
Maintenance
CCDB/MC
iTC Operation

복합기 cPP 개발 동향

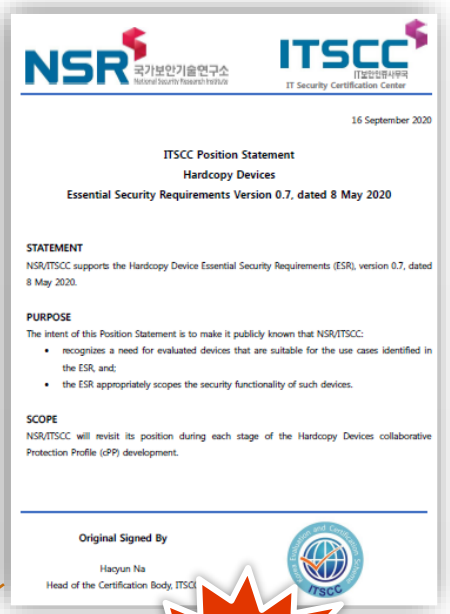
비휘발성 저장매체 '완전삭제' 또는 '암호화'

비휘발성 저장매체*	미•일 양자간 PP		IEEE PP	
	완전삭제	암호화	완전삭제	암호화
내장 형태	없음	없음	의무(잔여 정보 제거)	없음
탈착 형태	선택(이미지 오버라이트)	의무	의무(잔여 정보 제거)	없음

* HDD, SED(FDE), SSD, eMMC, Flash, SD Card, USB Stick, EEPROM 등 다양함

구분	명칭
인증 기관	한국, 일본, 스웨덴, 미국
업체	HP, Lexmark, Oce, Canon, Xerox, Ricoh, Konica, Fuji Film, Toshiba, Sharp, Riso, Seijo Expson, Kyocera
평가 기관	한국, 일본, 스웨덴, 미국, 캐나다, 호주

* 기타: 컨설턴트, 협회 등 참여


NSR 국가보안기술연구소 National Security Research Institute
ITSCC IT보안인증사무국 IT Security Certification Center

16 September 2020

ITSCC Position Statement
Hardcopy Devices
Essential Security Requirements Version 0.7, dated 8 May 2020

STATEMENT
NSR/ITSCC supports the Hardcopy Device Essential Security Requirements (ESR), version 0.7, dated 8 May 2020.

PURPOSE
The intent of this Position Statement is to make it publicly known that NSR/ITSCC:
- recognizes a need for evaluated devices that are suitable for the use cases identified in the ESR, and;
- the ESR appropriately scopes the security functionality of such devices.

SCOPE
NSR/ITSCC will revisit its position during each stage of the Hardcopy Devices collaborative Protection Profile (cPP) development.

Original Signed By
Hacyun Na
Head of the Certification Body, ITSCC

2018 2019 2020 2021 2022 Goal!

- (10.) CCDB HCD WG 승인(한국, 일본)
- (12.) HCD WG ToR, Work Plan 작성 (한국)

- (3.) HCD ESR 초안 작성 (한국)
- (3.) ESR 합의 (한국, 일본)
- (4.) HCD 업체 협의
- (8.) HCD iTC 승인 by CCDB

- (2.) HCD iTC 채택 by CCMC
- (5.) PS 발표
- (7.~9.) iTC 내부용 HCD cPP, SD (1차)
- (10.~11.) iTC 내부용 HCD cPP, SD (2차)

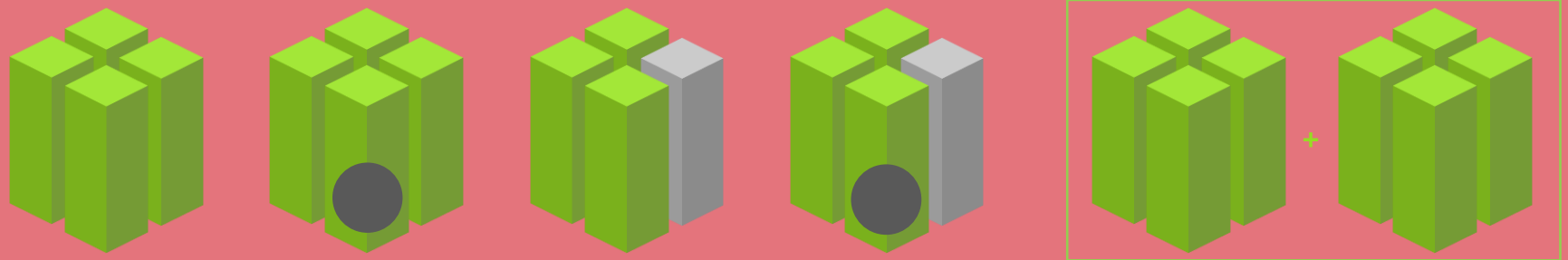
- (6.~8.) iTC 내부용 HCD cPP, SD (3차)
- (10.) 공개검토용 HCD cPP, SD (1차)
- (12.) 공개검토용 HCD cPP (2차)

- (3.) 공개검토용 HCD SD (2차)
- (7.) HCD cPP, SD 완료 (예정)
- (미정) ES 공개

준수 → 도입

TOE | 기술 및 해석 | 신규 접근법 | EAL

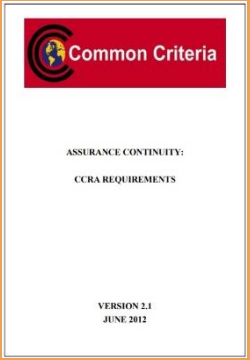
- TOE(Target of Evaluation)
  - 설명서가 제공되는 소프트웨어, 펌웨어 및/또는 하드웨어 집합
  - IT제품, IT제품 일부분, IT제품들의 집합, 제품으로 만들어지지 않는 특별한 기술, 또는 이들의 조합
  - PP 준수 시 준수 방법(Exact/Strict/Demonstrable)에 따라 TSF/non-TSF 정의가능
  - 서비스는 대상에서 제외됨



CCRA 협정에 따른 평가•인증 특징(2)

TOE | 기술 및 해석 | 신규 접근법 | EAL

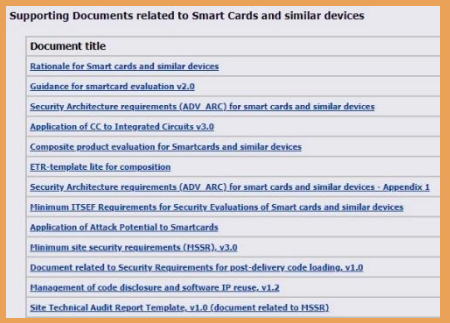
- CEM(Common Evaluation Methodology)의 엄격한 적용
  - 추가적인 해석은 제공할 수 있으나 확장(extension) 또는 정교화(refinement) 제한
- 보조문서(SD, Supporting Document) 적용
  - CCDB/MC의 승인을 득한 Mandatory 및 Guidance 보조문서 적용
- CCDB 중심의 기술 현안 합의 절차 준수



Assurance Continuity

Certificate Validity

cPP SDs



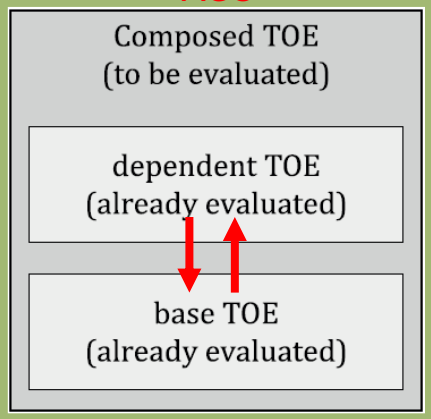
Smartcards SDs

CCRA 협정에 따른 평가•인증 특징(3)

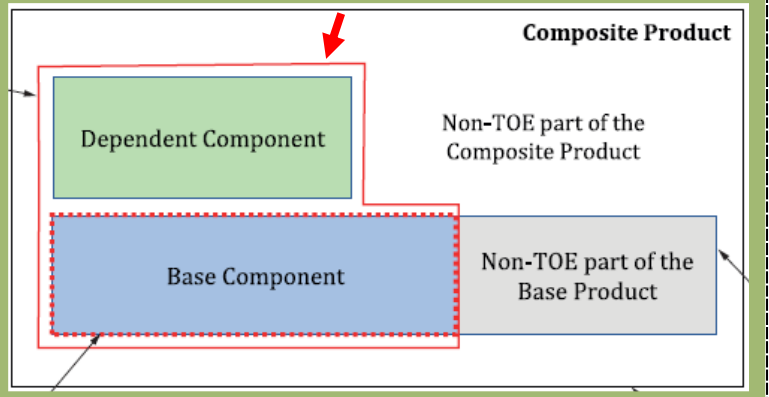
TOE | 기술 및 해석 | 신규 접근법 | EAL

- 모듈화된 평가방법론 제공
  - Base_PP, PP_Module, PP-Configuration
- 다양한 합성평가(Composite Evaluation) 방법론 제공
  - ACO, *_COMP
- Multi-Assurance Evaluation (차기 버전 CC/CEM)

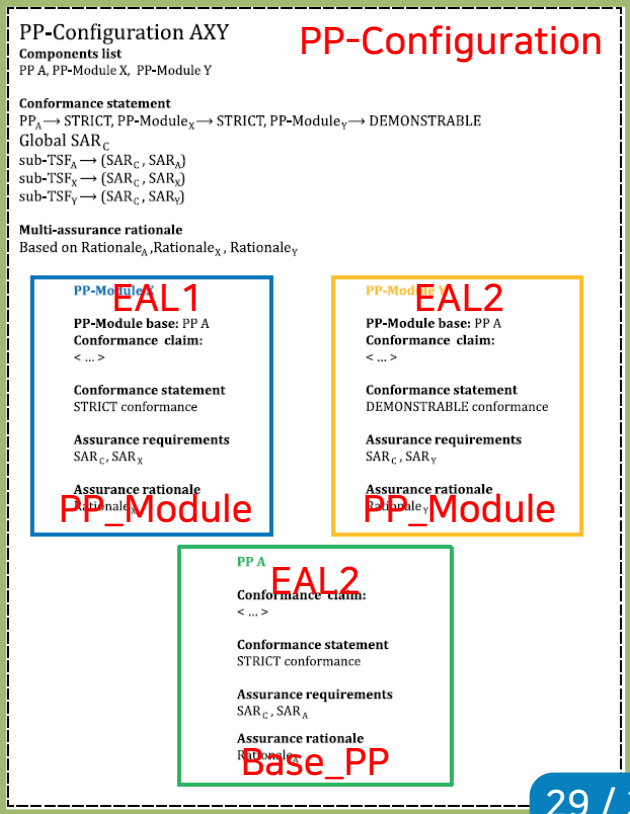
ACO



*_COMP



PP-Configuration



CCRA 협정에 따른 평가•인증 특징(4)

NSR

TOE | 기술 및 해석 | 신규 접근법 | EAL

- EAL(Evaluation Assurance Level)
  - 높은 EAL로 평가할수록 신청기관 및 평가기관의 노력, 시간, 비용 증가
- 개정 CCRA 협정
  - 비용효율성을 제고하기 위해 합리적인 상호인정 범위 지향(EAL2 이하)
  - EAL 등급에 기반한 불필요한 마케팅 경쟁 지양
- EAL1(+) 수준의 cPP 지향

보증 제출물 작성 가능?

평가 가능?

	TOE	ST(Low Assurance)	형상관리	사용자 운영 설명서	준비 절차서	기능명세서
신청기관						
평가기관	ATE_IND.1 AVA_VAN.1	ASE	ALC_CMC.1 ALC_CMS.1	AGD_OPE.1	AGD_PRE.1	ADV_FSP.1

CCRA 회원국 인증제품 동향

iPhone App for Authentication

File Storage and Sharing

New Generation Radio Access Network System Solution

Bluetooth Access Control System

Multi-factor Authentication

Digital Tachograph

Storage Management

Waste Bin Identification System

SDK

Physical Unidirectional Data Diode

Device Use and Application Execution Control

Secure Eraser (Tool, Module)

Contents Filtering Gateway

SBC(Session Border Controller)

Smart Meter

Crypto Module

Centralized Access Control to the Web Sites

Backup and Recovery Solution

Hardware IP Encryptor

Management Tools

Layer 1/Layer 2/Layer 3/Layer 4 Encryptor

IT Products/Systems Audit (Monitoring of Configuration)

Independent Security Subsystem in the SoC

Certificate Authority

Secure Audio Switch

CC is a Toolbox!

Video over IP

국가보안기술연구소

감사합니다