TPM 2.0 Security Evaluation Trust and Confidence

TCG Security Evaluation Work Group September 2017

Presentation outline

- SEWG publications
- **Common criteria** scheme overview
  - TPM 2.0 Protection profile
- Common criteria Evaluation scope
- **FIPS 140-2** overview
  - FIPS guidance for TPM 2.0 evaluation
- Leveraging certified TPM products
- Questions and answers

TCG Security Evaluation WG Public documents

Published documents

- TCG Protection Profile PC Client Specific TPM Family 2.0 Level 0 Version 1.0 (for TPM 2.0 Revision 1.16)

  https://trustedcomputinggroup.org/wp-content/uploads/TCG_PP_PC_client_specific_TPM_SecV2_v10.pdf

- TCG FIPS 140-2 Guidance for TPM 2.0 Version 1.0 Revision 1.0

  https://trustedcomputinggroup.org/wp-content/uploads/TCG_FIPS_140_Guidance_for_TPM2_0_v1r1_20170202.pdf

TCG draft document in Public Review (Sept 12 -> Nov 10)

- TCG Protection Profile PC Client Specific TPM 2.0 Version 1.1 (for TPM 2.0 Revision 1.38)

  https://trustedcomputinggroup.org/wp-content/uploads/TCG_PP_PC_client_specific_TPM_SecV2_v1.1_r12a_END_NOV10_PR.pdf

TCG Certification Program for PC Client TPM

- PC client TPM certification is built on 2 quality criteria

Interoperability

  - Functional compliance Vs specifications
  - Evidence: TCG compliance test suite pass results

Security

  - Evaluation compliant with **TCG TPM Protection profile**
  - Evidence: Common criteria certificate

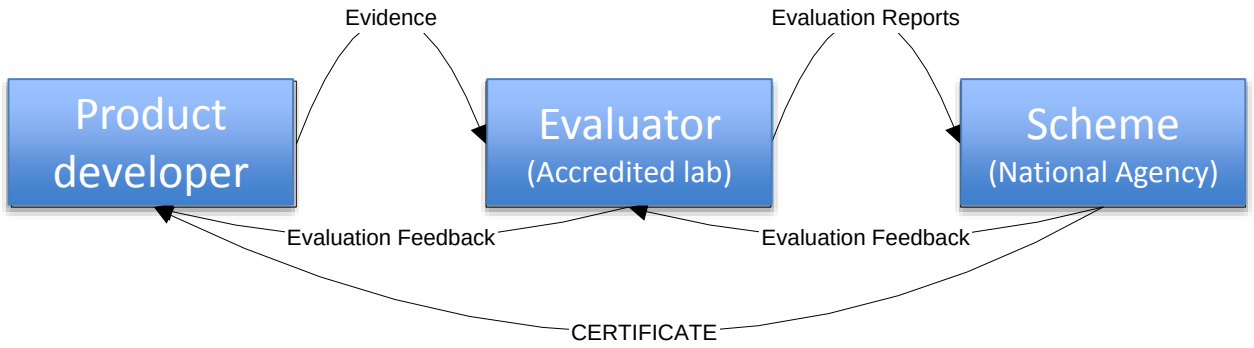
- List of certified PC Client TPMs is available on TCG Website

A (too) short introduction to

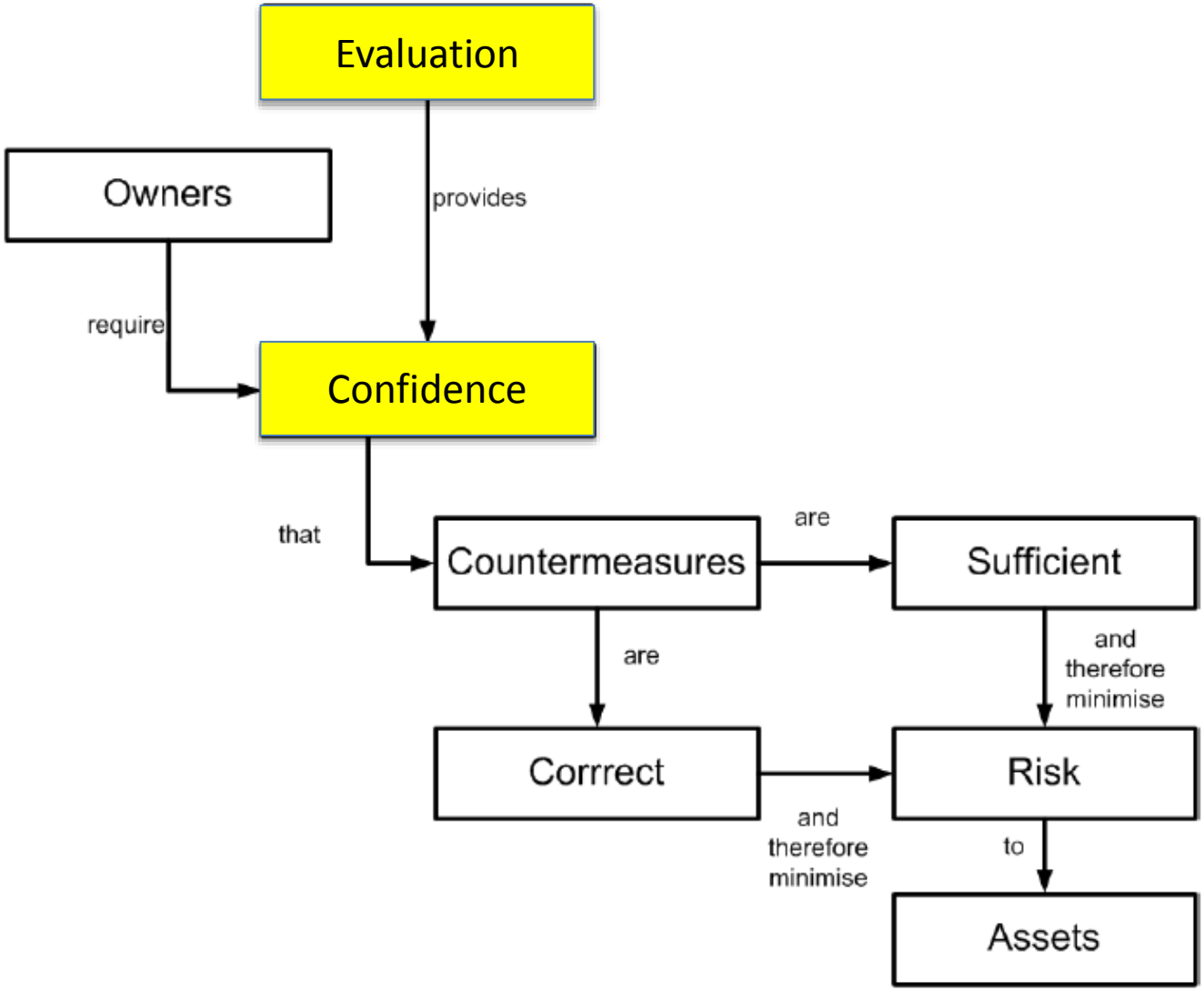
COMMON CRITERIA

What is Common Criteria?

- International Standard (IS0 15408) for the independent evaluation of the security of IT products
- Current version = CC3.1 R5 (April 2017)
- Standardised Security Requirements tailorable to fit security services
- Predefined scale of Evaluation Assurance Levels (EAL1 to 7)
- Two-level evaluation: accredited lab and scheme
- Mutual Recognition between national schemes (CCRA)
- Has its own terminology and acronyms

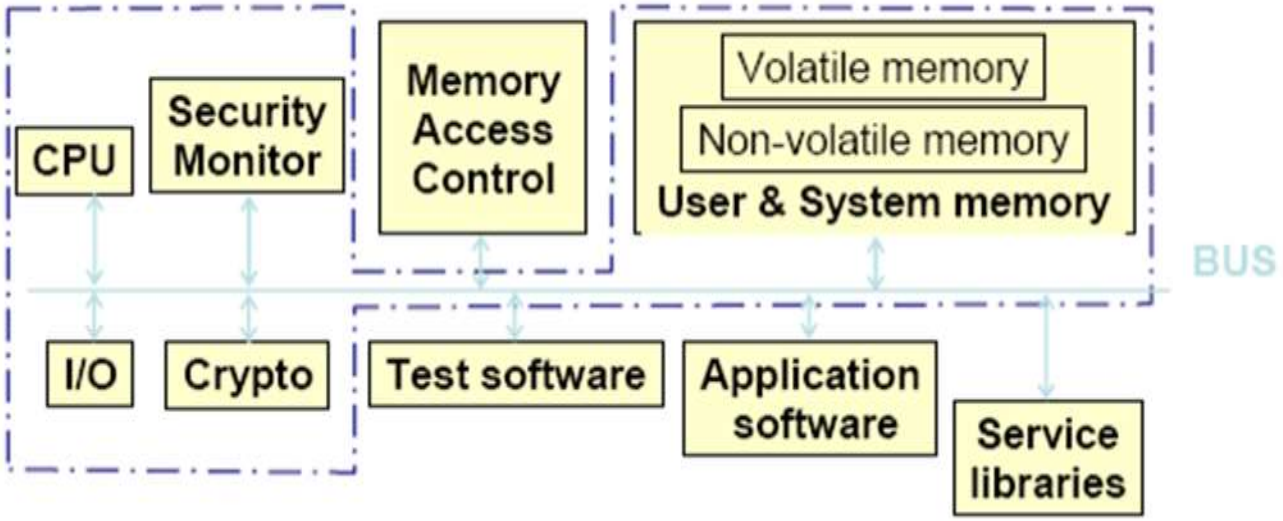


CC evaluation concepts



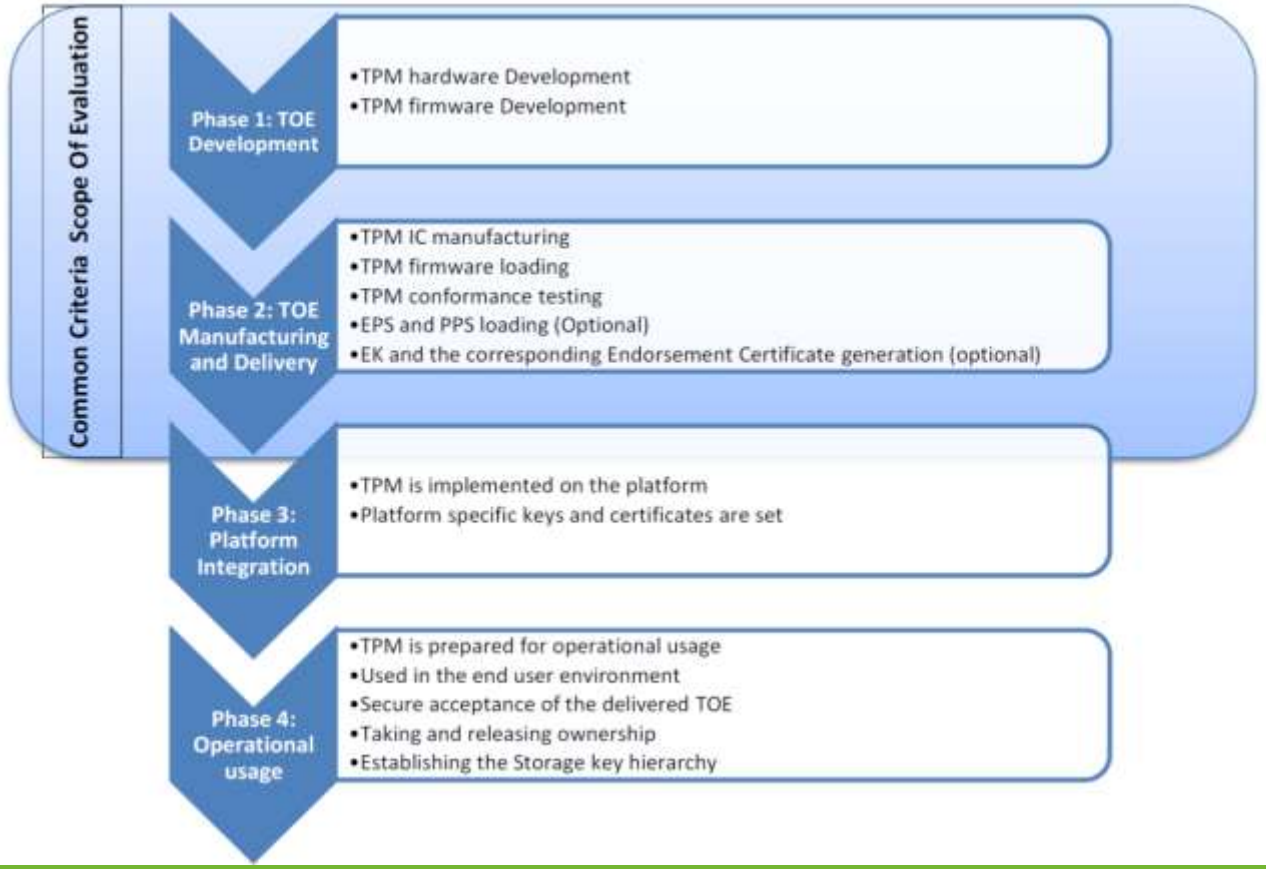
Target Of Evaluation

- **Target of Evaluation** (TOE) – has technical limits
  - Defines the evaluation boundary of the product.
  - Everything outside the TOE is in the environment



Scope of Evaluation

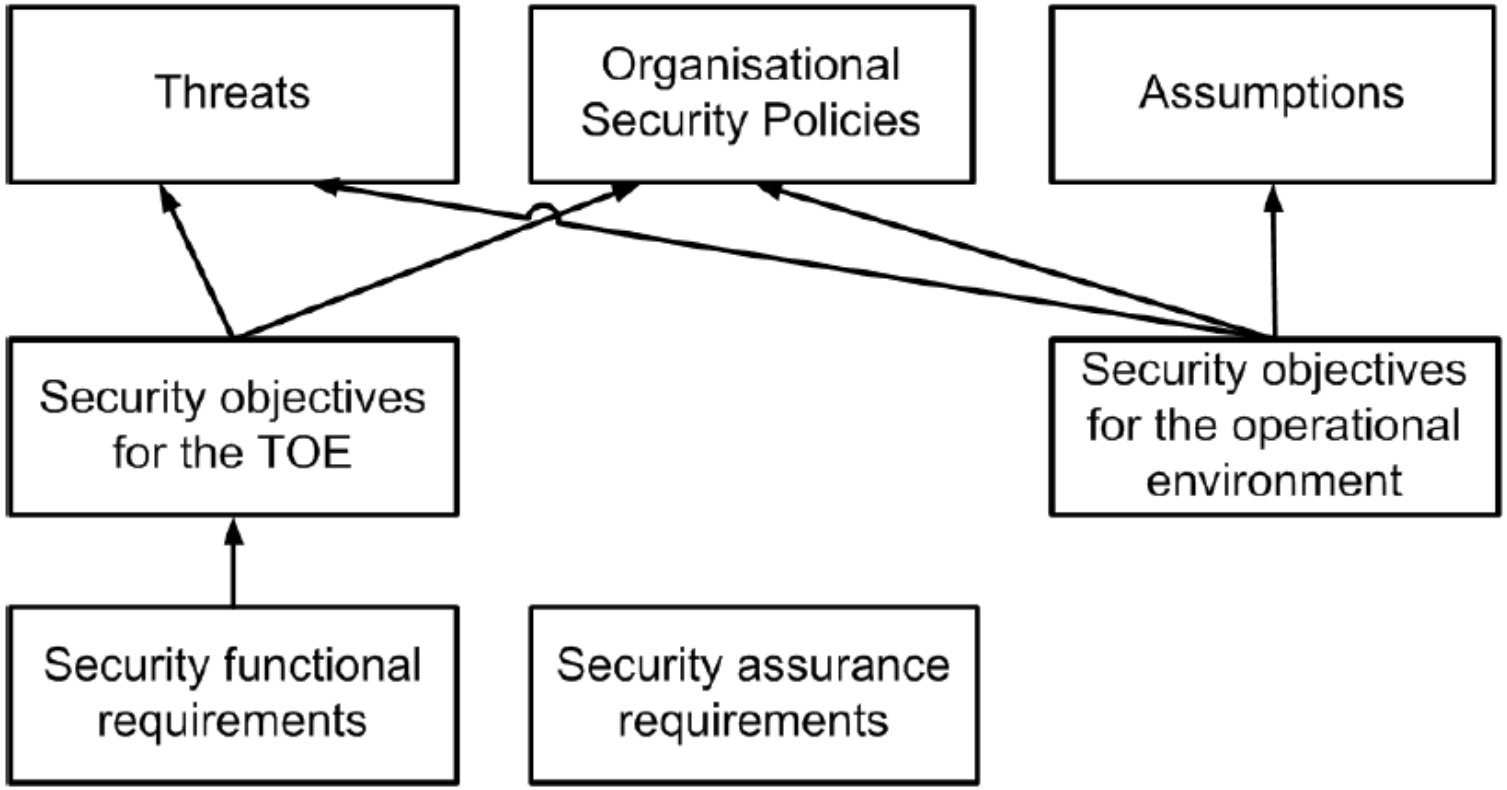
- **Evaluation Limit**
  - Defines the point at which the TOE is no longer under the control of the developer/manufacturer – based on the lifecycle of the product.



Protection Profile & Security Target

- **Target Of Evaluation (TOE)** - the product or system that is the subject of the evaluation.
  - "*set of software, firmware and/or hardware possibly accompanied by guidance*"
- **Protection Profile (PP)** - a document, typically created by a user or user community, which identifies security functional and assurance requirements relevant for a particular product. A PP effectively defines a class of security devices (Printers, Firewalls, TPMs..)
  - « implementation-independent statement of security needs for a TOE type »
- **Security Target (ST):** the document that identifies the security properties of the target of evaluation. Each target is evaluated against the security **functional** and **assurance** requirements defined in the ST.
  - Security target may claim compliance to a specific PP (or a set of PPs)
- TCG protection profile defines minimal set of security requirements to get TCG certification

PP contents: security problem definition, objectives and requirements



8 Organisational Security Policies

1. Context Management
2. Policy autorisation
3. Locality
4. Root of Trust for Measurement
5. Root of Trust for Reporting
6. Root of Trust for Storage
7. Field Upgrade
8. Elliptic Curve Direct Anonymous Attestation

TPM 2.0 PP Threats & Objectives(extracts)

Most objectives are linked to TPM 2.0 functional services.
The ones below focus on non functional security objectives:

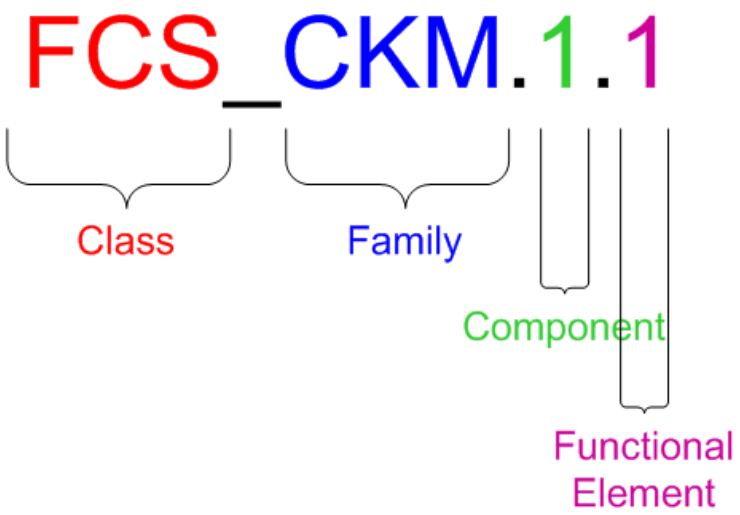
Threats	Description	Objective
T.Hack_Crypto	Incorrect cryptographic implementation leading to key compromise	O.Crypto_Key_Man
T.Hack_Physical	Unauthorized disclosure of TOE assets by hostile user by physically interacting with the TPM	O.Tamper_Resistance
T.Leak	Information exploited to disclose confidential assets	O.Tamper_Resistance
T.Insecure_State	The TPM may start or enter insecure state allowing an attacker to obtain sensitive data	O.Fail_Secure
T.Residual_Info	Data scavenging	O.No_Residual_Info

Functionality and Assurance

- Security Assurance provides confidence that Security Functionality meets its Security Objectives
- Therefore CC defines two types of security requirements:
  - Security Functional Requirements (SFR): the “what?”
  - Security Assurance Requirements (SAR) the “how?”
- Evaluation Assurance Levels (EAL) define coherent set of Security Assurance requirements
  - EAL gives a global assurance level for an evaluation

Security Functional Requirements

- SFRs: a translation of the security objectives of the TOE into a standardized language.
- CC 3.1 Part 2 defines 11 classes containing 65 families of SFRs
- SFRs are assigned a standard identifier:



- SFRs are also organized with dependencies to have a common and coherent approach for all evaluations

SFR example from CC Part 2 tailored for TPM2.0 PP

Underlined text has been added to match TPM 2.0 specifications

FCS_COP.1/RSASign Cryptographic operation (RSA signature generation/verification)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSASign The TSF shall perform signature generation and verification[31] in accordance with a specified cryptographic algorithm RSASSA_PKCS1v1_5, RSASSA_PSS[32] and cryptographic key sizes 2048 bit[33] that meet the following: PKCS#1v2.1 [26][34].

SFR Example from TPM 2.0 PP

FIA_AFL.1/Recover Authentication failure handling (recovery)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1/Recover The TSF shall detect when maxTries[64] of unsuccessful authentication attempts occur related to unsuccessful password or HMAC authentication attempts for

(1) objects where DA is active (i.e. noDA attribute is CLEAR)
(2) NV Index where DA is active (i.e. the TPMA_NV_NO_DA attribute is CLEAR)[65].

FIA_AFL.1.2/Recover When the defined number of unsuccessful authentication attempts has been met[66], the TSF shall block the authorisations for RecoveryTime seconds[67].

The counter failedTries is incremented when the authentication attempt failed. The counter failedTries is decremented by one after recoveryTime seconds if:

(1) the TPM does not record an authorisation failure of a DA-protected entity,
(2) there is no power interruption, and
(3) failedTries is not zero.

The counter failedTries is reset to 0 by

(1) command TPM2_Clear()
(2) TPM2_DictionaryAttackLockReset() with lockoutAuth or lockoutPolicy.

Security Assurance Requirements (1/3)

- **Security Assurance Requirements** (SARs) are descriptions of how the TOE is to be evaluated
- Detailed descriptions for the evaluator of the measures taken during development and evaluation of the product to assure confidence with the claimed security functionality.
- For example, an assurance level may require that all source code is kept in a change management system, or that full functional testing is performed.
- The Common Criteria provides a catalogue of these SARs
- The requirements for particular targets or types of products are documented in the ST and PP, respectively

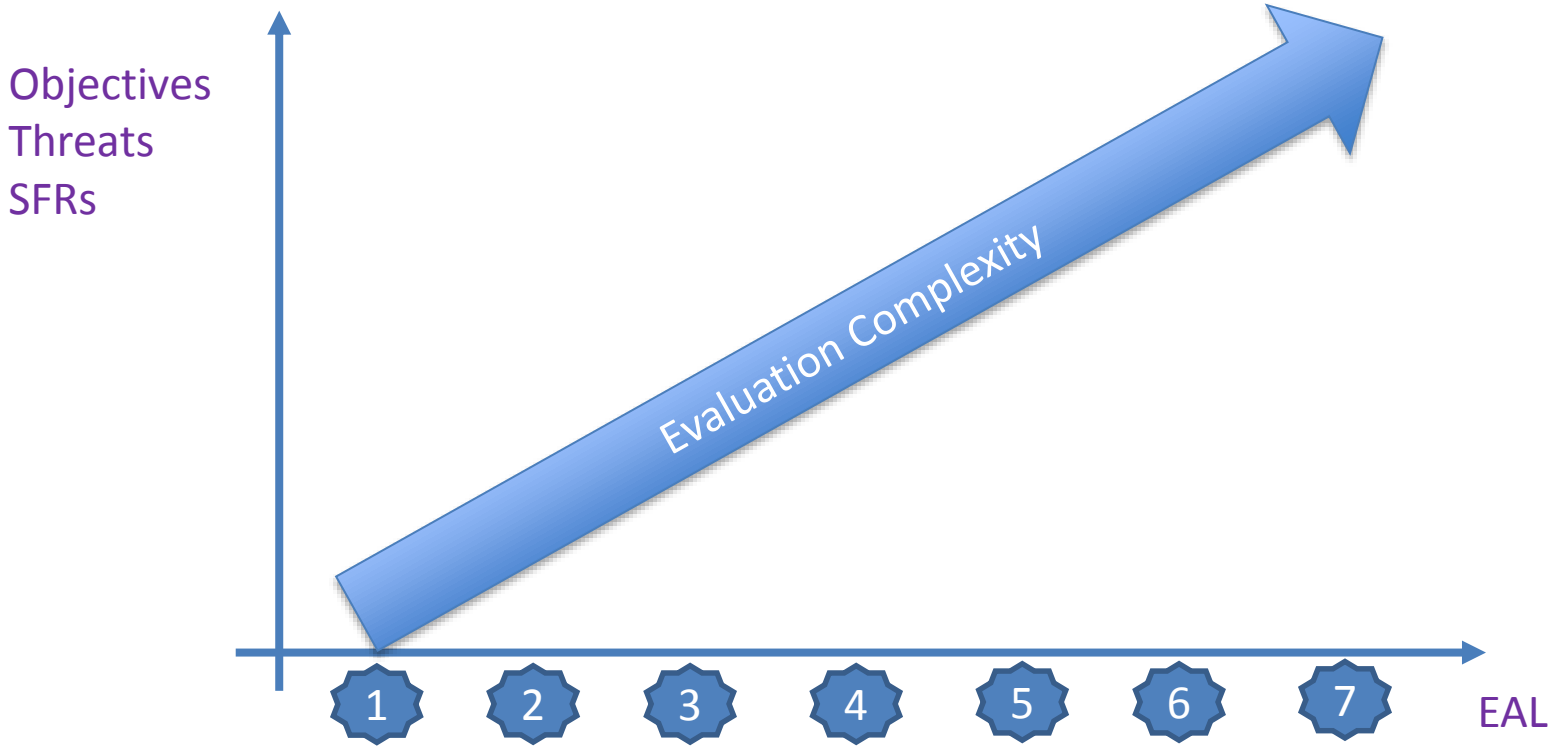
Assurance Classes (2/3)

- ADV – Development
  - Including design and production process of TOE
- AGD – Guidance Documents
- ALC – Lifecycle Support
  - Including Configuration management, development security, tools & techniques, product lifecycle, flaw remediation
- ATE – Tests
- AVA – Vulnerability Assessment
- ASE – Security Target Assessment
- For PP only: APE – Protection Profile Assessment

Evaluation Assurance Levels (3/3)

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Evaluation complexity



Assurance level selection must match market expectations but also system complexity.

TPM 2.0 PP Assurance level

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

1

Augmentations
-> EAL4+

Vulnerability Analysis

- SFR FPT_PHP.3: (fullfilling O.Tamper_Resistance)

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing [assignment: *additional physical tampering scenarios*][86] to the TSF[87] by responding automatically such that the SFRs are always enforced.

- AVA_VAN.4: resistance to moderate attack potentials

How to refine evaluation methodology?

- What kind of attacks the product must resist to?
- What's the link between attacks and assurance levels?
- Attack evolutions security watch?

CC supporting documents for evaluations

- CCDB-2013-05-002 :
  Application of Attack Potential to Smartcards (version 2.9)
- Mandatory document for CC evaluation
  - used for certified products
- Attack rating depending on several factors
  - Elapsed time
  - Expertise
  - Knowledge of the TOE
  - Access to the TOE: number of samples (production or test)
  - Equiment
- Vulnerability level « AVA_VAN.x » mandates that TOE must be resistant to attacks up to a specific range.

Vulnerability Analysis Methodology

- 1st step: the identification of potential vulnerabilities;
  - In-depth code/vhdl review
    - Compliance to design documents and claimed countermeasures
    - No malicious code, no forgotten bypass functions
- 2nd assessment to select attacks scenarios .
- 3rd penetration testing to determine whether the identified potential vulnerabilities are exploitable in the operational environment
  - Fault injections: Glitches, Laser, …
  - Side Channel Attacks - Leak
    - SPA: Static Power Analysis
    - DPA: Differential Power Analysis
    - And others
  - Reverse engineering – Physical hacking
    - TOE modification

Security Attack Watch: SOGIS

- Security is a continuous race
  - New attack paths appear (Academic papers, Lab, University)
  - New attacks appear (Labs, Hackers)
- SOGIS: group of European countries, CCRA members subset
  - Including Japan and Turkey as Liaison member
- Security watch is covered by one SOGIS working group: JHAS
  - JHAS audience not limited to SOGIS – specific registration process
- Joint Hardware Attack Subgroup holds meetings
  - Attendence: Vendors, Labs, National schemes, other certification scheme (EMVCo)
  - Meeting every 2 months
  - Follow-up of the new attacks or rating of existing attacks.
  - Public document available in « Application of Attack Potential to Smartcards »
  - Evaluation methodology details are shared between JHAS members

CC Recognition Agreement

Certificate Authorizing Members

Certificate Consuming Members

CCRA recognition and Industry requirements

- Up to recently automatic recognition was up to EAL4
  - No evaluation methodology agreement above
- Nowadays, certificate Recognition between CCRA countries is automatic but limited up to EAL2 (+ALC_FLR)
  - EAL4+ (ALC_FLR) if Collaborative Protection Profile
- TPM PP targets **EAL4+** (ALC_FLR & AVA_VAN.4)
  - > CCRA recognition covered up to EAL2 (+ALC_FLR)

Collaborative PP and International Technical communities

- Issue: several PPs exist for the same kind of device.
- Proposal: 1 technical committee endorsed by CC unique per device
- **Collaborative Protection Profile (cPP):**

  A *Protection Profile* collaboratively developed by an ***International Technical Community*** endorsed by the ***Management Committee***.

  A *cPP* and related *Supporting Documents* define the minimum set of common security functional requirements and the *Achievable Common Level of Security Assurance*.

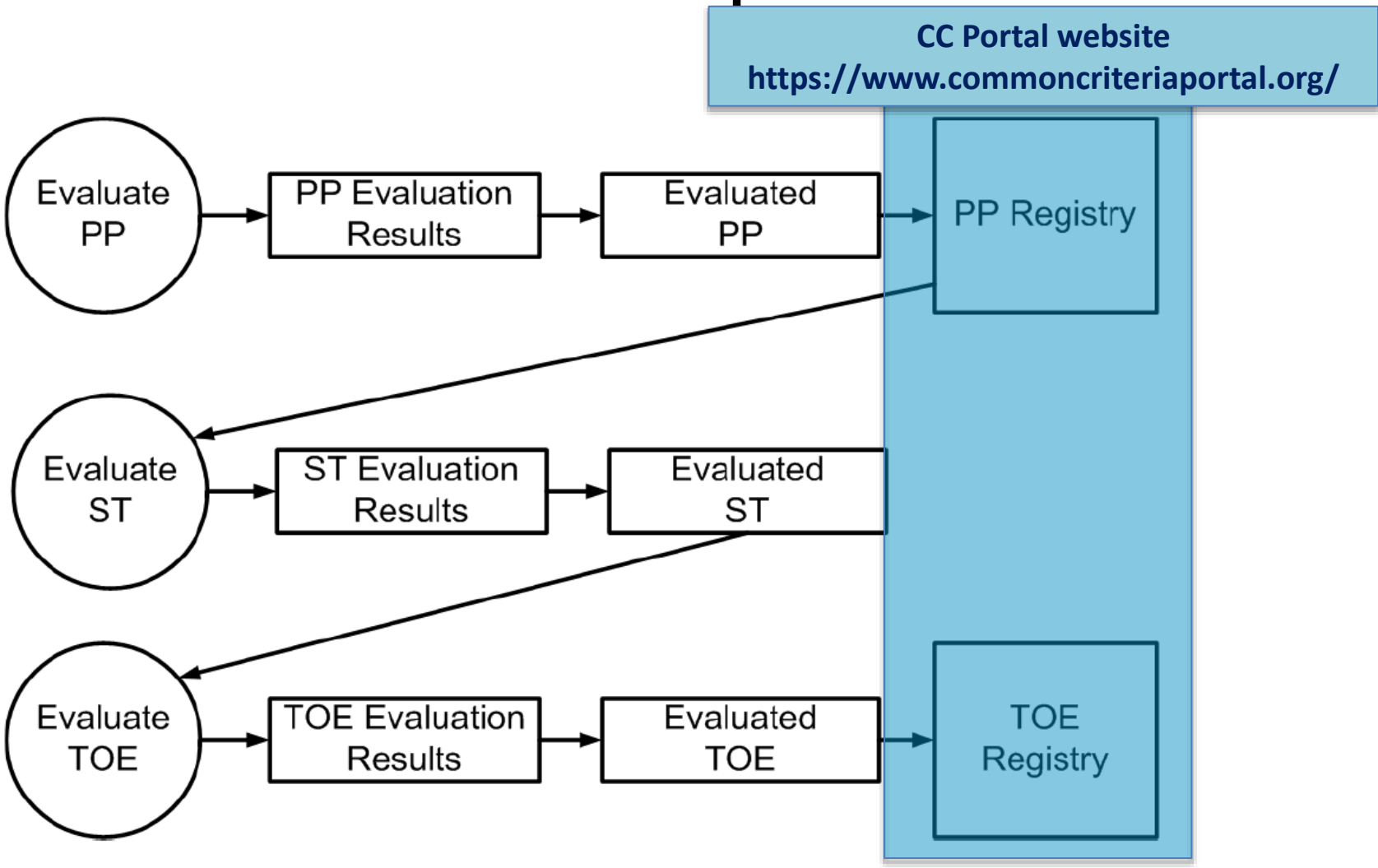
  It addresses vulnerability analysis requirements to ensure certified products reach an *Achievable Common Level of Security Assurance*.

- **International Technical Community (iTC):**

  A group of technical experts including *Participants*, *Certification/Validation Bodies*, *ITSEFs*, developers and users

- Several cPPs are under edition – See Common Criteria website

Evaluation results publication



Automotive thin TPM 2.0 Protection Profile

- *Strict conformance* to a PP mandates that TOE implements all SFRs and all SARs from the PP
- Automotive thin platform profile is a subset of the PC Client Profile -> all SFRs may not be implemented
  -> PC Client PP not usable for evaluation of Automotive thin implementations
- Automotive thin protection profile modifcations at a glance:
  - Removal of SFRs linked to optional features in automotive thin
  - Field upgrade is kept as optional package
  - SARs are kept unchanged

FIPS 140-2

FIPS 140-2 CMVP (short) overview

- FIPS 140-2 defines a set of generic security requirements and security services formalization requirements for products evaluation
  - Cryptographic Module Specification
  - Cryptographic Module Ports and Interfaces
  - Role, Service and Authentication
  - Finite State Model
  - Operational Environment
  - Cryptographic Key Management
  - EMI/EMC (if applicable)
  - Self-Tests
  - Design Assurance
  - Mitigation of other attacks (optional)
- FIPS 140-2 defines 4 compliance levels with different quality criteria
- Product features described in a « **Security Policy** » public document
  - Available on FIPS CMVP Certified Product List

Level based Criteria

Security Requirements

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical se and optio	Role-base operator a	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using man entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

TPM 1.2

TPM 2.0

TPM 2.0

FIPS 140-2 CAVP

- Cryptographic Algorithm Validation Program
  - Correct implementation of approved cryptographic algorithms
  - Cryptographic interoperability between FIPS certified products
- Process
  - CAVP generates test vectors
  - Vendors receives test vectors and generates test answers
  - CAVP validates test answers and assign certificates for each algorithm
  - Vendor includes certificate numbers in the Security Policy

TCG SEWG deliverables

- SEWG released a guidance to help TPM vendors and Evaluation labs for the evaluation of TPM 2.0 implementations
- Target level: 2
- Main goals were
  - to factorize standard behaviour description in a form suitable for security policy
    - E.g. Key management, Selftests, …
  - to anticipate conflicts between TPM specifications and FIPS requirements
    - TPM 1.2 lessons learnt
  - to provide additional information regarding TPM optional features becoming mandatory for FIPS requirements fullfillment

LEVERAGING CERTIFIED TPM FOR SYSTEM EVALUATION

CC System certification

- CC certified TPM simplifies System CC evaluation
- Protection profile reusable SFRs
  - Cryptographic Services (Including random generator)
  - Storage, Measurement, Reporting
- TPM assets protection configuration
  - TPM services are already covered by TPM evaluation
  - System architecture has to describe the settings of the security attributes of TPM assets to comply with platform security functions
- System assets protection (TCG use cases)
  - Define Platform assets
  - Describe how platform assets are protected by TPM security functions

System Security Target

FIPS System Certification

- FIPS certified TPM simplifies system FIPS evaluation
- Cryptographic features reusable
  - **Cryptographic algorithm certificates**
    - **Including FIPS approved random generator**
  - Storage, Measurement, Reporting
- TPM assets protection configuration
    - TPM services are already covered by TPM evaluation
    - System architecture has to describe the settings of the security attributes of TPM assets to comply with platform security functions
- System assets protection (TCG use cases)
    - Define Platform assets
    - Describe how platform assets are protected by TPM security functions

System Security Policy

THANK YOU

Any questions?