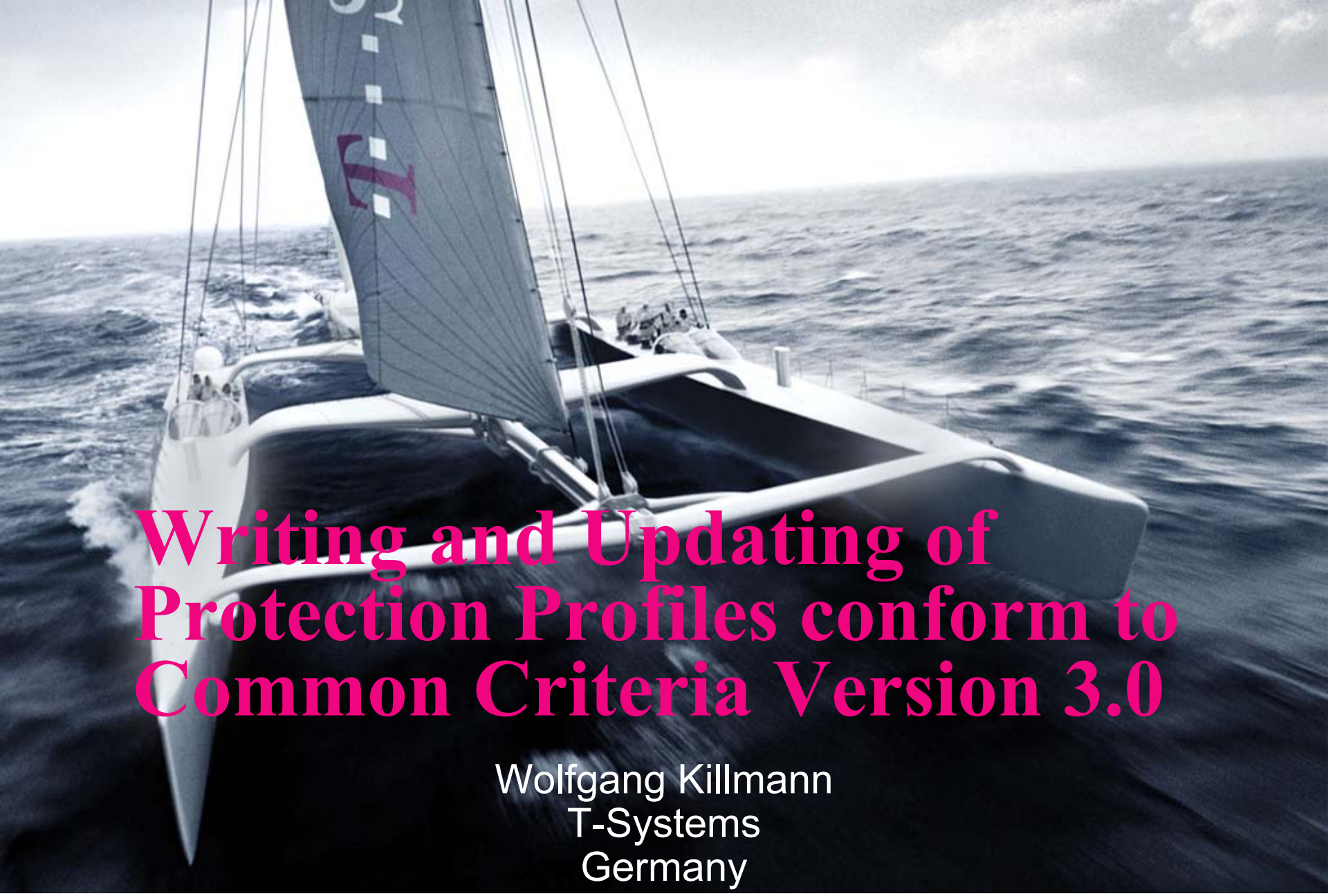


Writing and Updating of Protection Profiles conform to Common Criteria Version 3.0

Wolfgang Killmann
T-Systems
Germany

T · · Systems ·

Overview

Success story of protection profiles

PP conformance as defined in CC V3.0 part 1

New functional paradigm of CC V3.0 part 2 and security functional requirements

Security assurance requirements from PP prospective

Evaluation methodology and PP

Success Story of PP

CC concept of protection profiles is approved in practice and accepted by costumer

- 67 certified PP worldwide (July 2005)
- PP cover a broad range of technologies from smart cards up to mainframes
- some PP are referenced as official standards
- many PP are accepted as standards by consumers and vendors

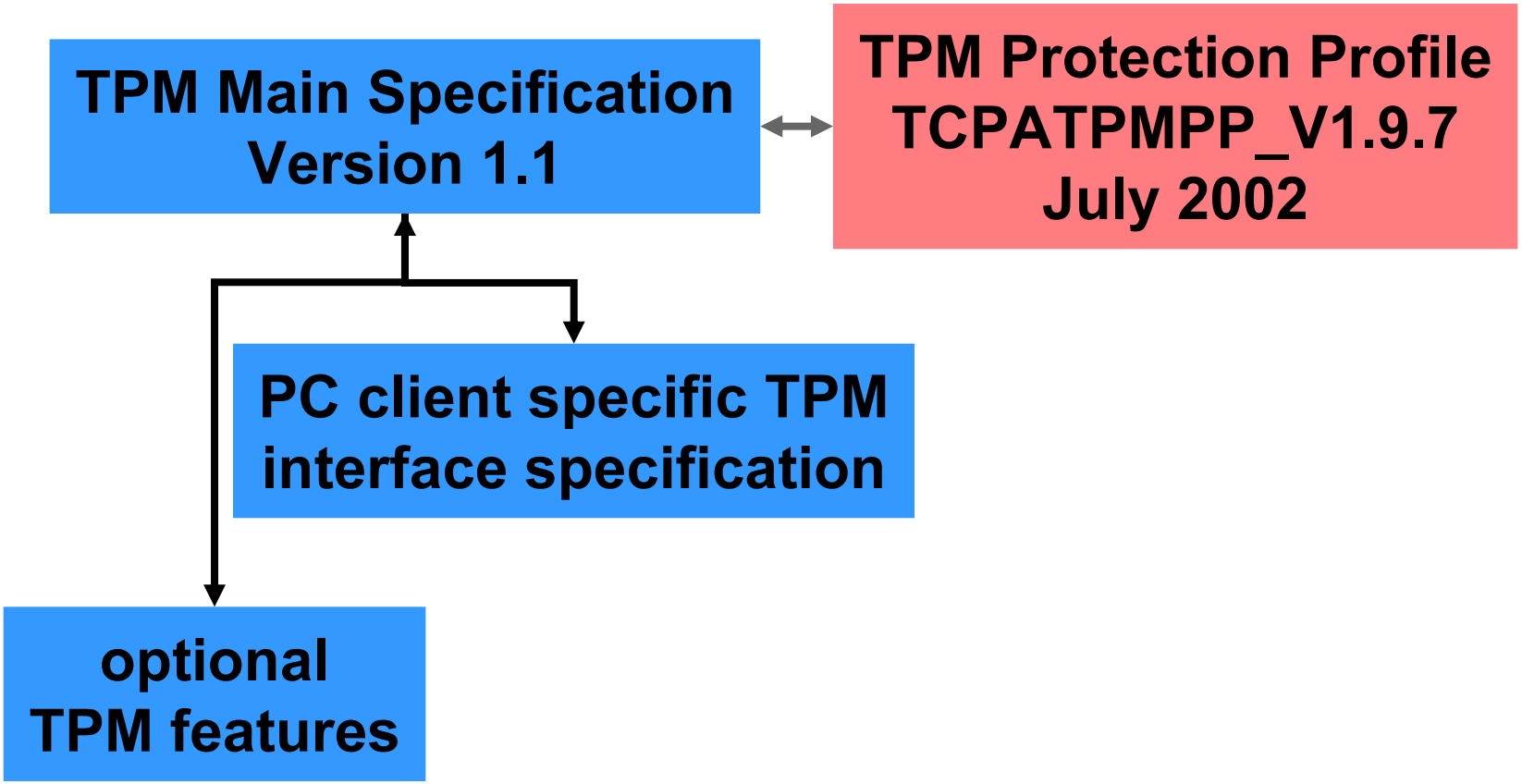
Success Story of PP

V3.0 changes CC significantly

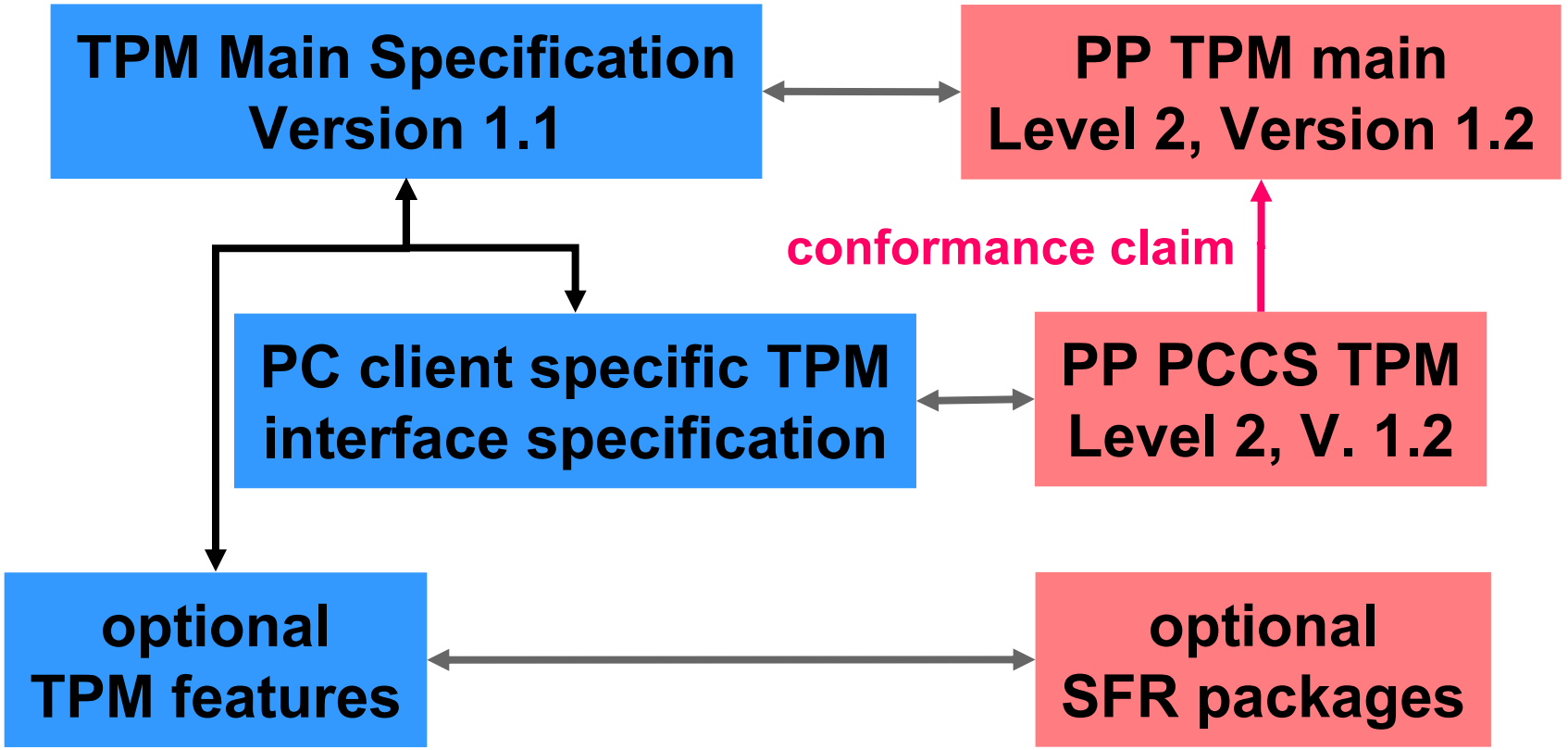
- CC V2.2 PP can not be used after transition period → PP shall be rewritten or updated for further use
- What advantages does CC V3.0 provide for PP development and use?
- What issues arise by updating the current PP to CC V3.0?

CC V3.0 Part 1 and PP
PP conformance in CC V2.2

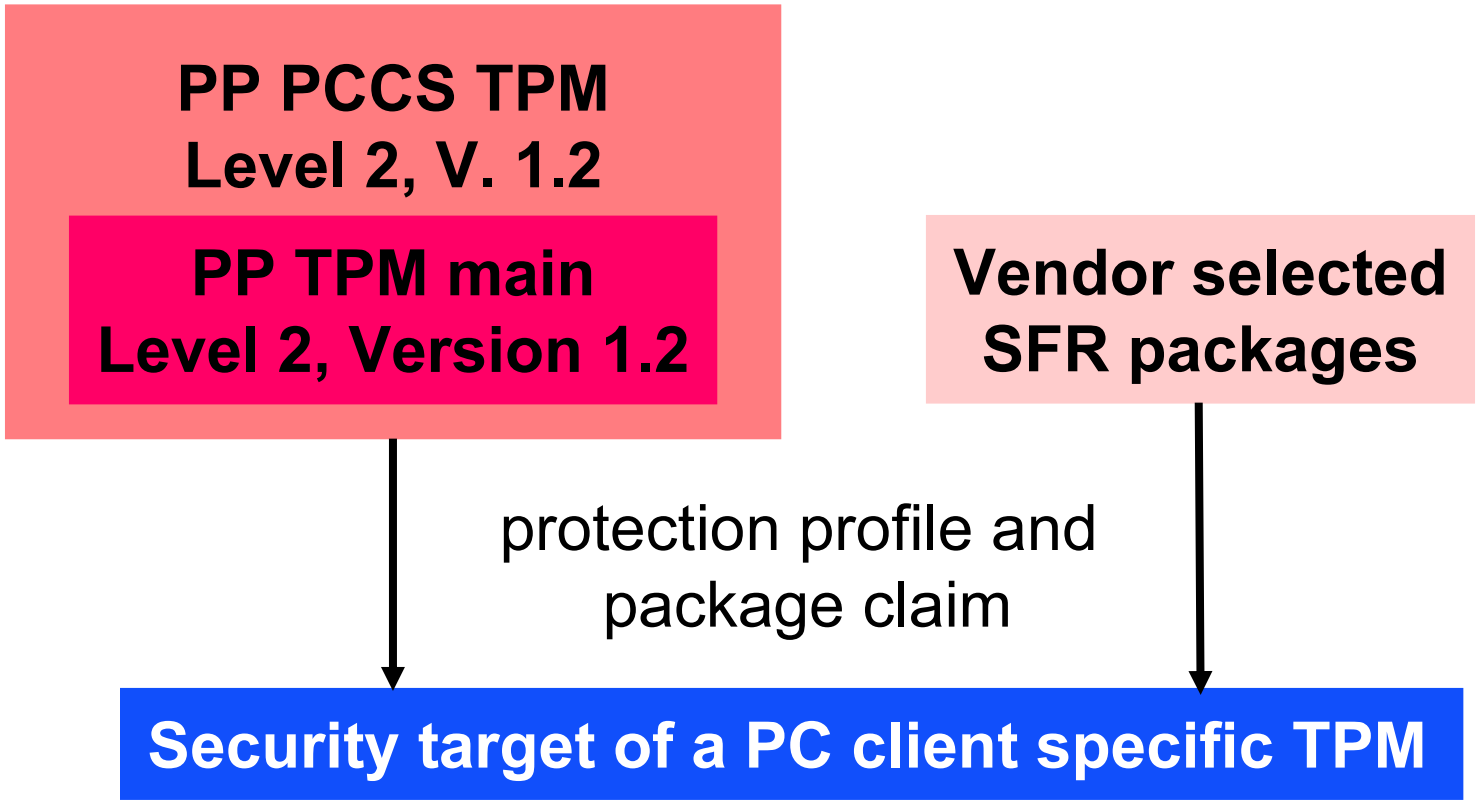
Trusted Computing Group (TCG) Trusted Platform Module (TPM)



CC V3.0 Part 1 and PP
PP conformance in CC V3.0

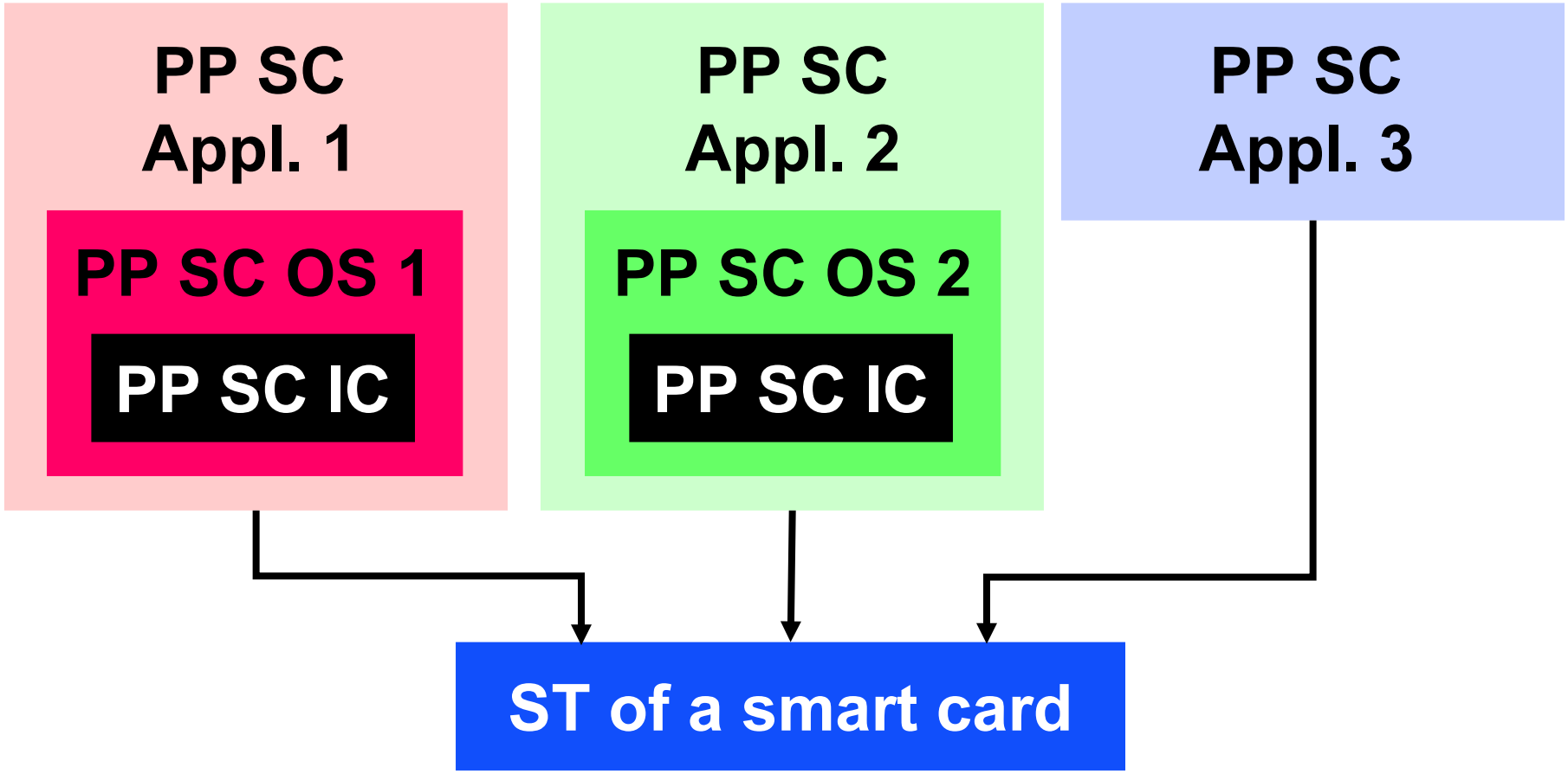


CC V3.0 Part 1 and PP
PP conformance of ST



CC V3.0 Part 1 and PP
PP and ST for composite Eval.

PP set for composite evaluations of smart cards (like Eurosmart PP set)



CC V3.0 Part 2 and PP
Functional Paradigm and SFR

PP TPM V1.1 (CC V2.2)

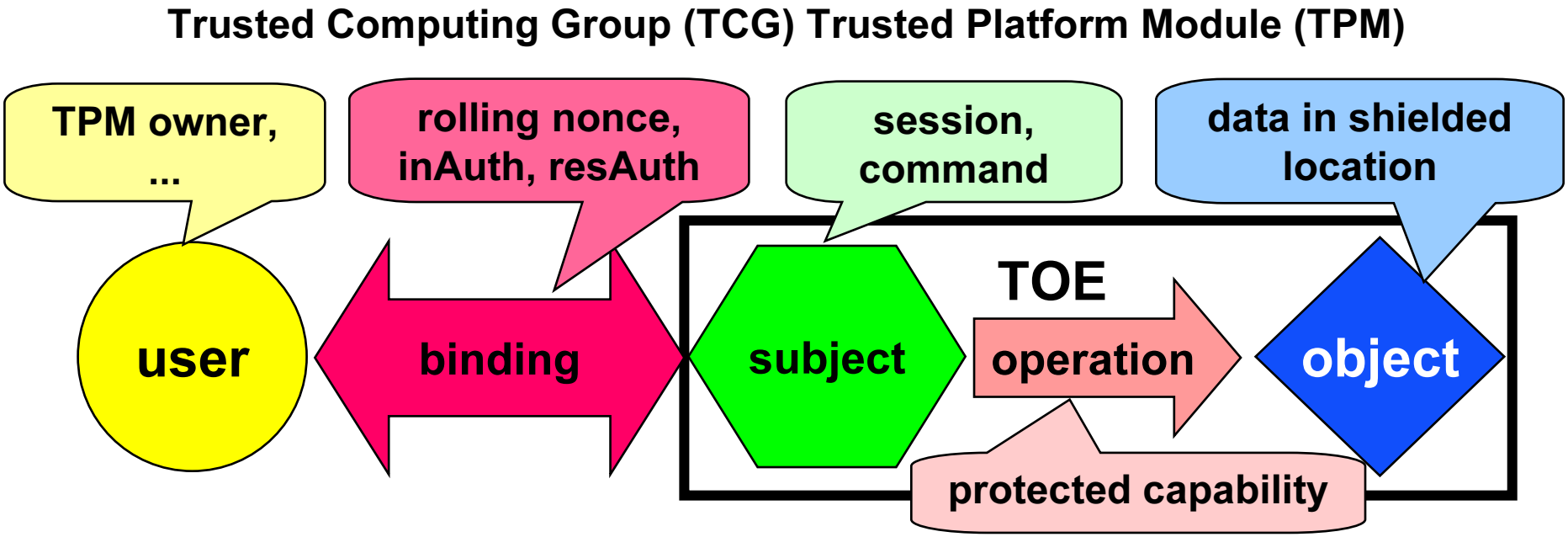
- requires cryptographic functions and access control to the related keys

PP TPM Level 2, V1.2 (CC V3.0)

- describes operations in the context of the Root of Trust for Measurement, Reporting and Storage
- addresses the cryptographic mechanisms to implement these operations

→ new functional paradigm encourages the PP writer for clear and precise description of the security functionality

CC V3.0 Part 2 and PP
Functional Paradigm



FIA_UAU.1.1 The TSF shall authenticate a user before the user can bind to

(1) OIAP authorization session,

(2) OSAP authorization session,

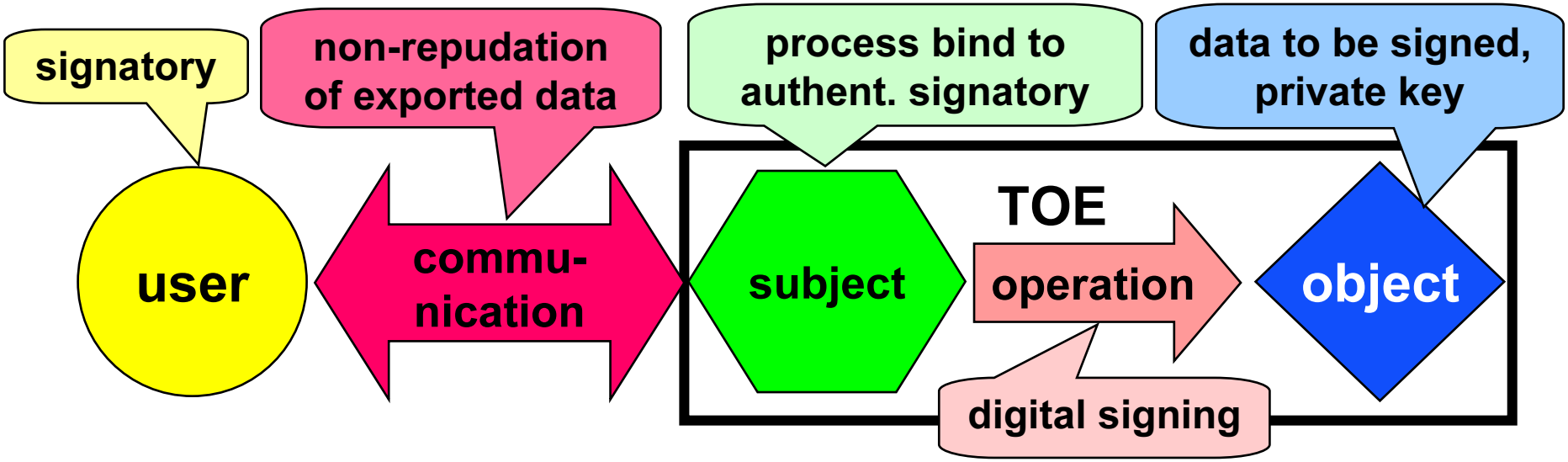
(3) DSAP authorization session,

(4) Commands which require authorization and are executed outside a authorization session [1].

[1] [assignment: *subject*]

CC V3.0 Part 2 and PP
FCS class removed

PP Secure signature-creation device, PP CM CSP signing operations



FCO_NRE.2.1 The TSF shall generate evidence **by digital signature according to the List of approved algorithms and parameters** to that *process using private key* [1] has exported *signed data* [2] to a user bound to that subject.

[1] [assignment: *subject*], [2] [assignment: *data*]

CC V3.0 Part 2 and PP
Extended components

PP writer may consider to define new functional components (extended components)

- new SFR for specific security functions
  - digital signature verification
- reuse of components of CC V2.2 part 2 if necessary
  - key generation FMI_CKG.1 (FCS_CKM.1)

CC V3.0 Part 2 & 3 and PP
SFR and SAR

CC V2.2 SFR address protection against compromise of internal secrets by illicit information flow

- PP used SFR components like FDP_IFC.1, FDP_ITT.1, FPT_ITT.1 or FPT_EMSEC.1 which are not contained in CC V3.0 part 2

- CC V3.0 deal with illicit information flow in AVA_VAN
  - precise SPD shall result in attack scenarios subject of the vulnerability analysis
  - related functionality is not traced trough ADV
  - protection should be reported to the consumer

CC V3.0 Part 3 and PP
Selection of EAL and Extensions

EAL of CC V2.2 and CC V3.0 are mostly compatible to each other from PP prospective

- If PP required FPT_PHP, FPT_RVM.1 and FPT_SEP.1 then reference monitor concept of ADV_ARC.1 is already included
- Removing AVA_SOF.1 in CC V3.0 result in an overall strength requirement by AVA_VAN even if distinguishing between strength of identified security function makes sense

CC V3.0 CEM and PP
Attack potential example CC V2.2

PP Secure signature-creation device

- assumed attack scenarios like this
  - **Identification**:
    elapsed time ≈ 1 day, proficient, public information,
    < 1 day access to TOE, standard equipment
  - **Exploitation**:
    elapsed time ≈ 1 day, proficient, public information,
    < 1 day access to TOE, standard equipment

  → 18 points = moderate attack potential

- PP requires resistant to high attack potential (AVA_SOF.1 high, AVA_VLA.4)

CC V3.0 CEM and PP
Attack potential example CC V3.0

Weighted parameters approach

- SSCD example → 3 points → basic
- layman, public knowledge, standard equipment, 6 month → 26 points
- expert, critical knowledge, bespoke equipment, 1 month → 24 points

Conclusion

→CC V2.2 and CC V3.0 may differ significantly

→this layman (with easy window of opportunity) may successfully attack TOE resistant to high attack potential

→elapsed time is overemphasized

CC V3.0 CEM and PP
Attack potential calculation

CEM V3.0 describes two new calculation methods of attack potential providing different results

- Weighted parameters approach
  high attack potential 15 – 26 points
- Independent factor approach
  high attack potential ≥ 34 (39) points

→ How to ensure ”repeatability and objectivity” of the evaluation results using these CEM V3.0 attack potential assessment approaches?

Conclusion

Current PP must be rewritten for use in CC V3.0 evaluations

CC V3.0 provide useful features for PP developers and users

CC V3.0 part 2 affects significantly the PP updates

CEM V3.0 attack potential assessment shall be revised to ensure repeatability, objectivity and mutual comparability of the evaluation results