Lessons learnt in writing PP/ST

Wolfgang Killmann
T-Systems

Overview of the talk

- Lessons learnt in writing PP/ST
  - Practical experience of PP/ST writing
  - Issues with and suggestions for PP/ST writing
- Conformance claim to PP
  - Use of conformance claims
  - Discussion of strict and demonstrable conformance
- Relation between functional and assurance requirements
- Resistance against attacks claimed in PP/ST
  - Understanding of attack potential
  - Different resistance against attacks within a product?

General aspects of PP usage

PP are widely used

PPs are issued by governmental organisations expressing legal requirements

- PP Secure signature-creation devices
  (developed by CEN, referenced by EU commission, BSI-PP-{0004,0005,0006})
- PP Machine readable traveller documents (MRTD)
  - Basic access control (FMI Germany, BSI-PP-0026-2006)
  - Extended access control (FMI Germany, BSI-PP-0026-2006)

PPs are developed by vendors to establish industrial security baseline

- PP Security integrated circuits
  (Eurosmart vendors group, BSI-PP-0002, BSI-PP-0035)
- PP PC client specific trusted platform module PC
  (PP PC specific TPM, Trusted Computing Group, BSI-PP-00??)

PPs may address security of specific IT product or IT system types

- eHealth smart cards, terminals, server (eHealth connector)

General aspects of PP usage
2 roles of PP

- PPs are issued to express minimum security requirements from user point of view. The PP developers
  - may follow the PP/ST guidance
  - often ask for help by CC specialists (as editor) to write their PP
- PPs are used to write STs for product evaluation. Therefore
  - CC part 1 describes the concept of PP and ST
  - PP have to meet the assurance class APE

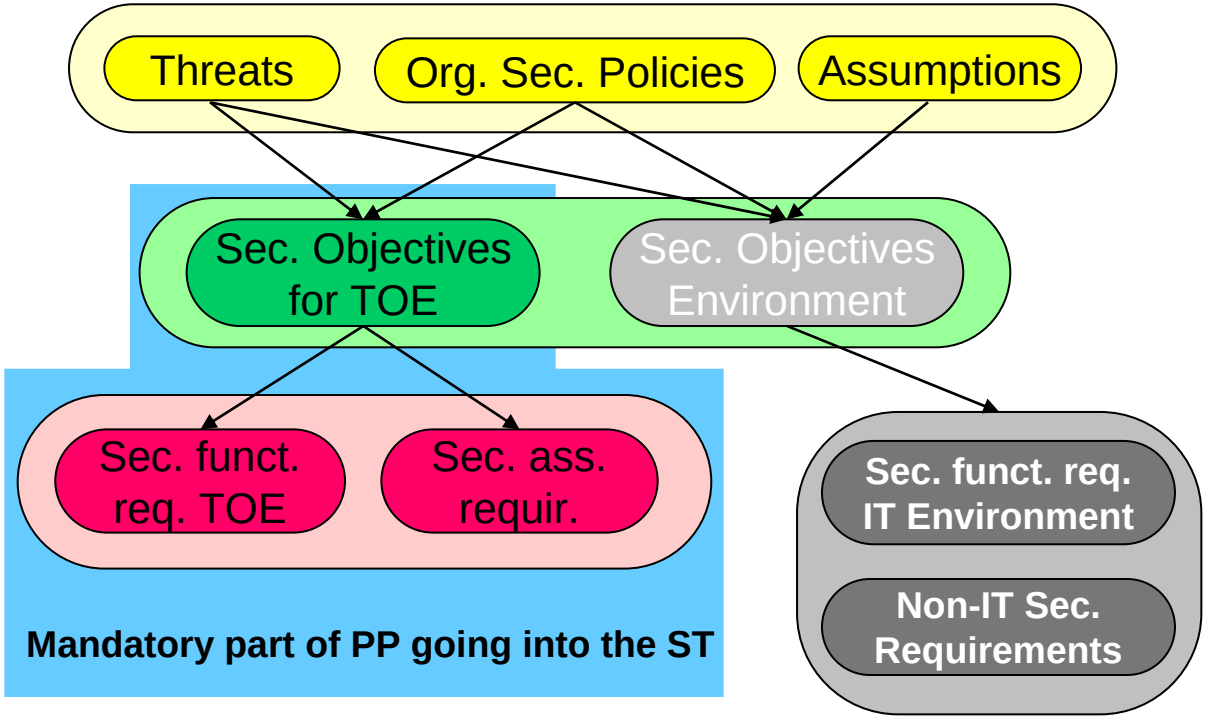
- These 2 roles are sometimes in conflict
  - PP should be easy readable for customers but CC are not easy to understand.
  - Strong concepts are necessary for evaluation but limit the applicability of PPs.
  - Open issues make development and application of PPs difficult.

Conformance claim

Mandatory parts according to CC version 2.3

If ST claims conformance the ST **shall include** from PP and **may extend** the PP parts

- security objectives (SO) for the TOE,
- security functional requirements (SFR) for the TOE
- security assurance requirements (SAR) for TOE

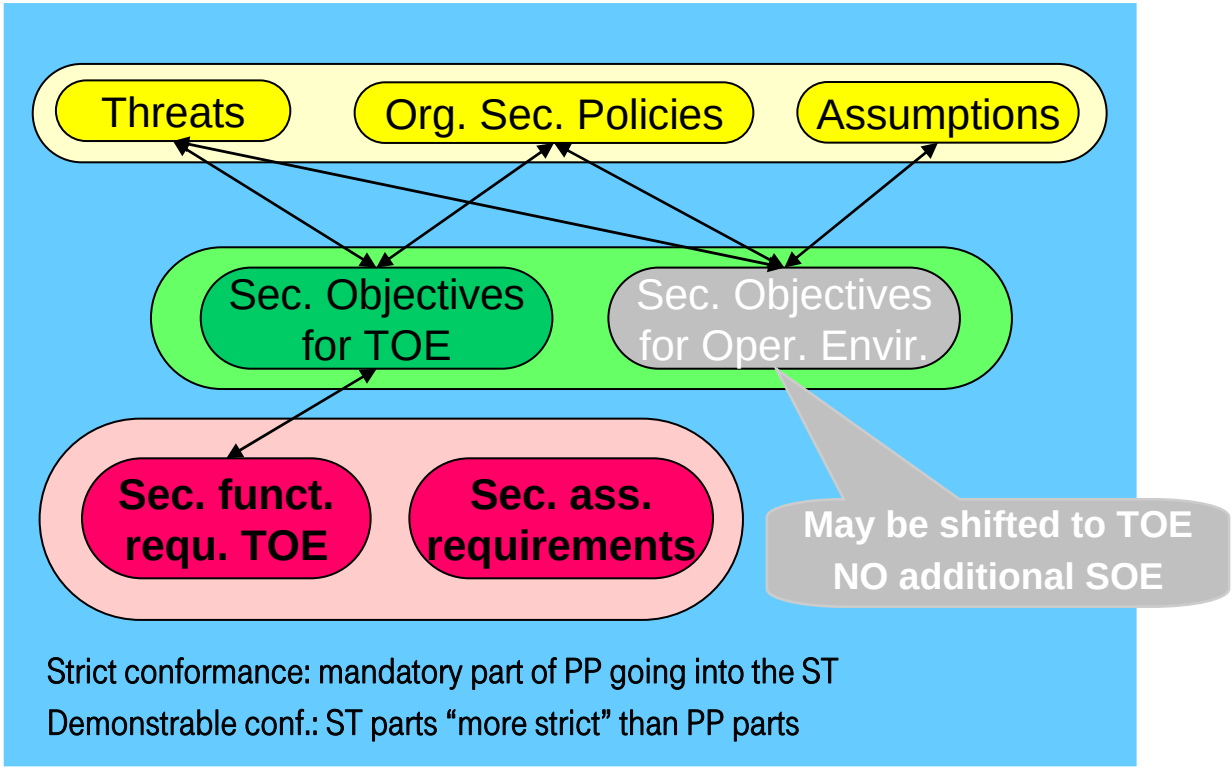


Conformance claim

Mandatory parts according to CC version 3.1

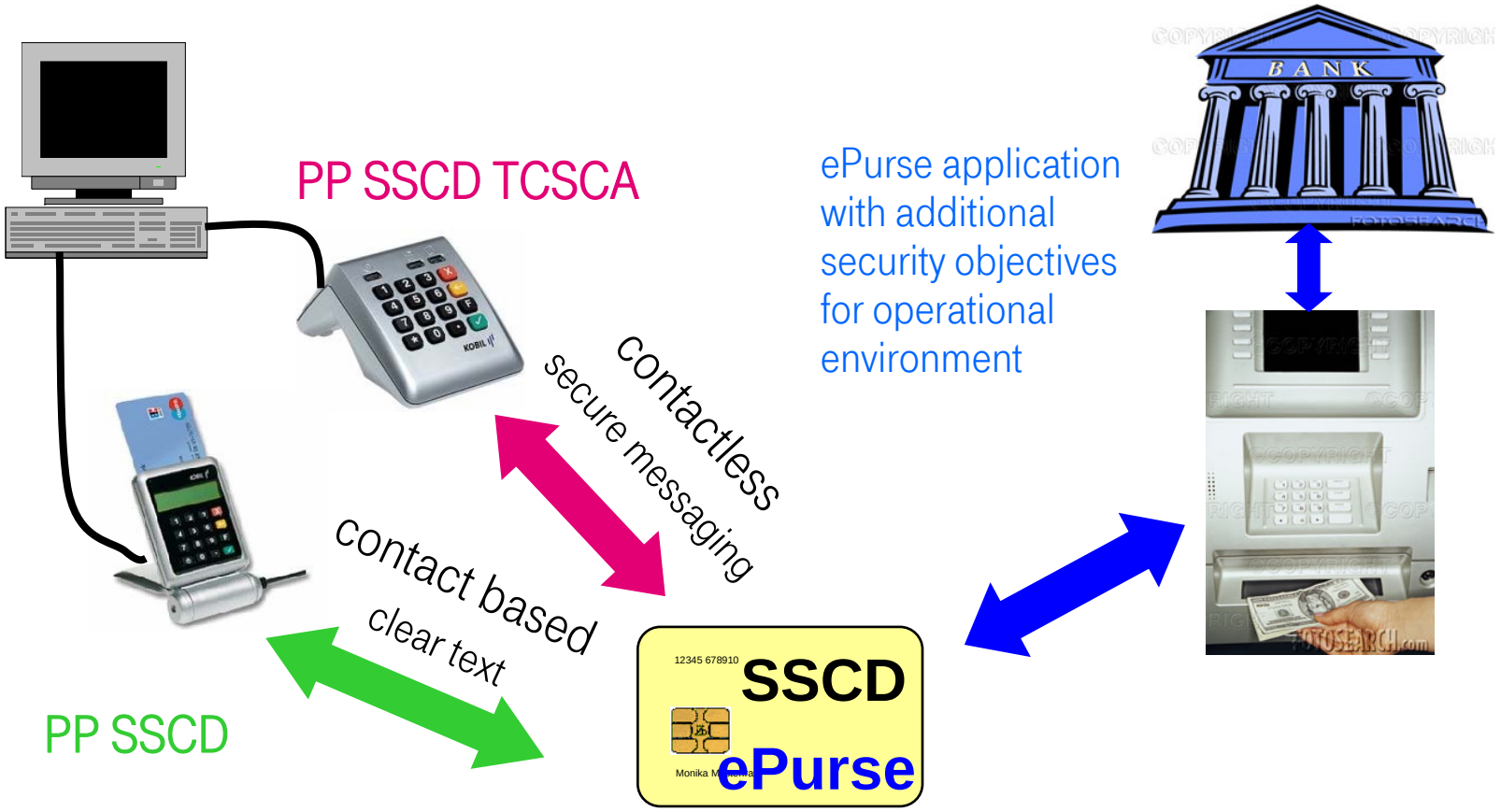
- PP may require **strict** or allow **demonstrable** conformance
- **strict**: mandatory
  - threats, policies, assumptions (SPD)
  - SO for the TOE,
  - security requirements for the TOE (SFR, SAR)

  forbidden to
  - modify assumptions,
  - add SO for operational environment
- **demonstrable**:
  - PP/ST provides rationale of being more restrictive than the claimed PP



Conformance claim

Example: PP secure signature-creation device



Shall we perform separate evaluations only because of changed environment?

Conformance claim

Issues and Suggestion for **strict** conformance claim

Issues of strict conformance (CC p1, sec. D2):

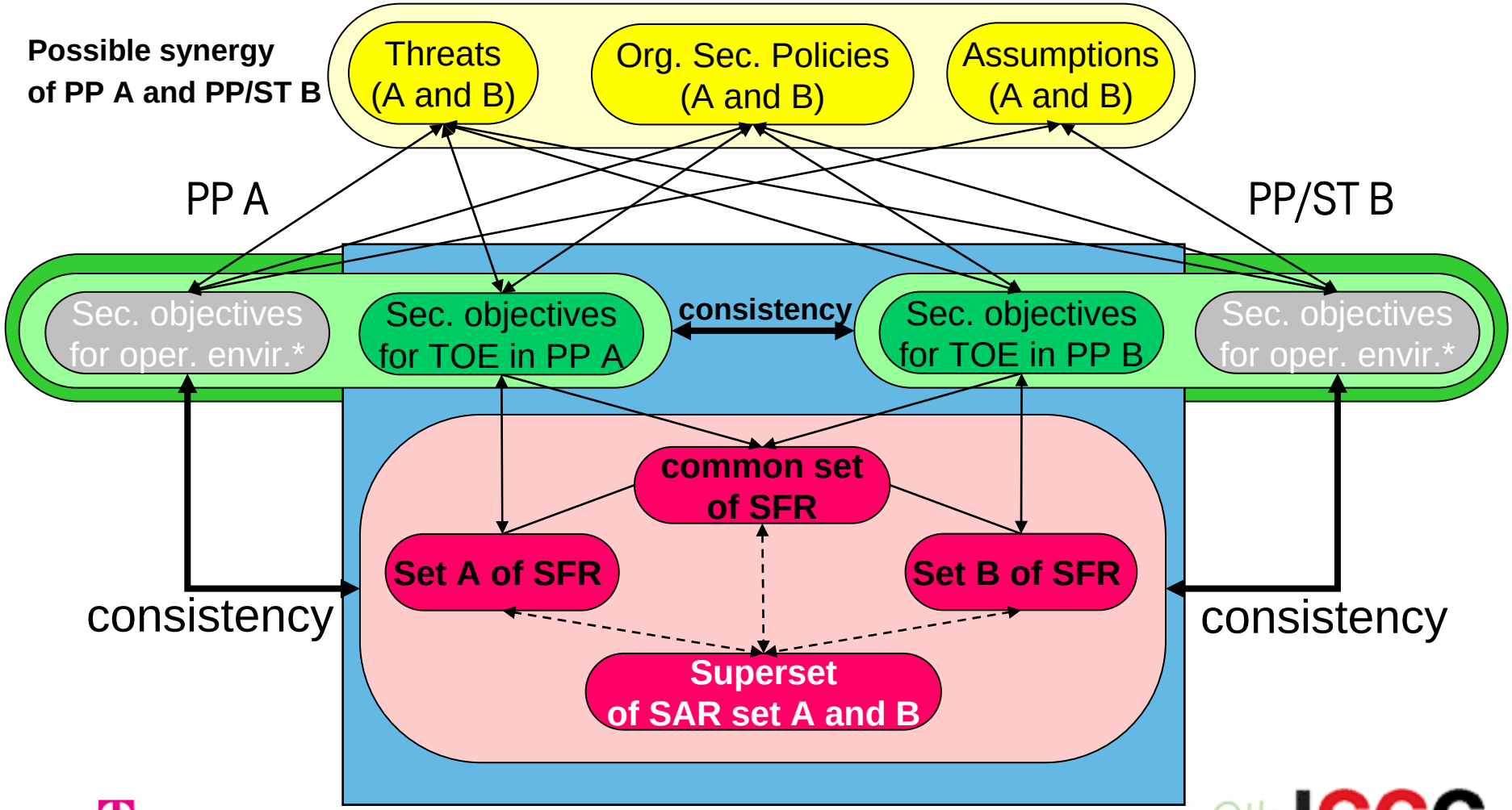
- over-defined (by SPD): conflicts if
  - TOE provides additional security services in the ST or
  - claiming conformance to additional PPs

Suggestion for **strict** conformance

- PP/ST claiming conformance to a PP shall include
  - all security objectives for the TOE
  - all security functional requirements
  - all (or hierarchically higher) security assurance requirements
- The security objectives for the operational environment **must not contradict** the security objectives for the TOE (consistency).
- The PP/ST may contain additional assumptions and security objectives for the operational environment if they relate to **additional security services** provided by the TOE of the PP/ST.

Conformance claim

Suggestion for **strict** conformance claim



Conformance claim

Suggestion for **demonstrable** conformance claim

Issue of demonstrable conformance (CC part 1, D.2)

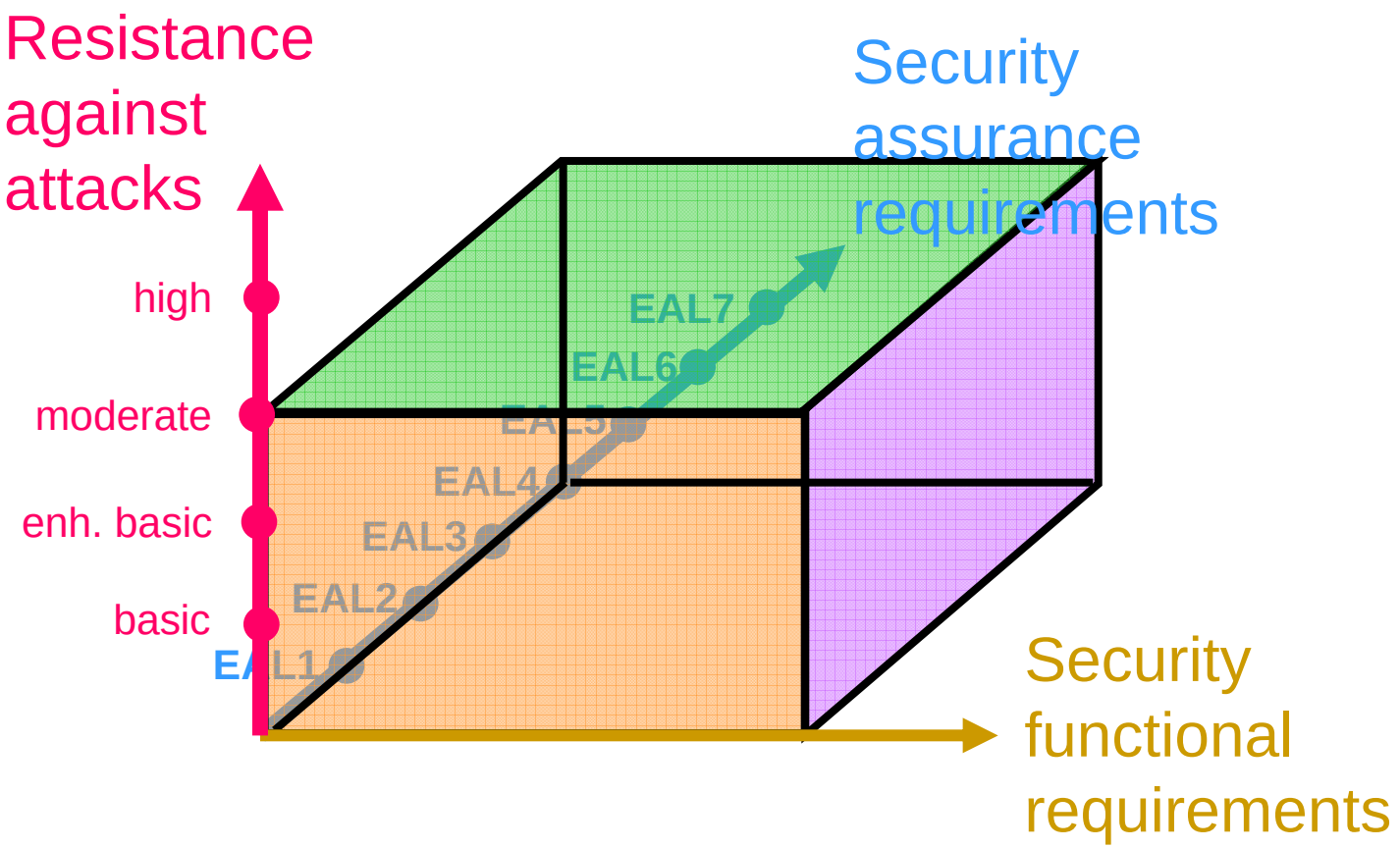
- “all TOEs that meet the PP also meet ST” (wrong)
- “all environments that meet SPD of PP also meet SPD of ST” (very strong)
- The criteria for “more restrictive” and the degree of freedom for “conformance rationale” are not clearly stated.

Suggestion for demonstrable conformance:

- Definition of rules how the rationale may demonstrate that all TOEs that meet the ST also meet the PP:
  - Set of SO for TOE in the PP/ST includes all SO for TOE in the PP.
  - For identified SO for TOE the PP/ST may define different SFR than the PP.
  - Set of SAR in the PP/ST includes all or hierarchically higher SAR in the PP.

Functional and assurance requirements

Which level of EAL and resistance to be claimed in PP/ST



Security functional requirements
Relation between PP/ST and specification

{APE,ASE}_REQ.2.7C:
SFR shall be suitable to meet the security objectives of the TOE.

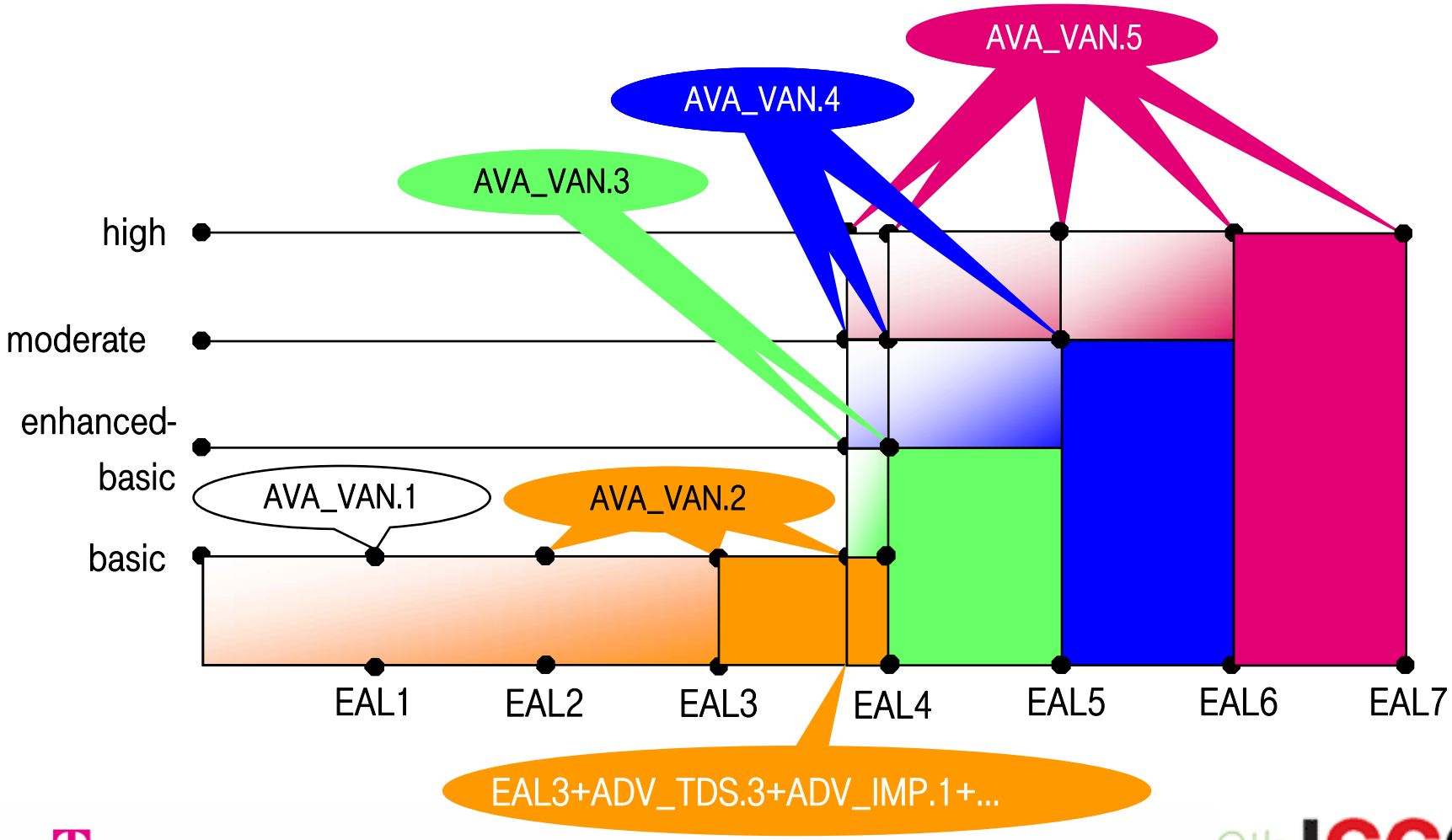
- This is rather a requirement but also a way to find the appropriate SFR.
- Example: PP Secure signature-creation device, PP MRTD, …

In some cases a **functional specification** is given and
the PP/ST writer has to reconstruct the SPD and the SO.

- Examples: PP PC client specific TPM, PP eHealth server, …
- Specifications aim on interoperability and describe functionality on ADV_FSP level, but typically without any SPD or SO. This result in issues of PP development:
  - How to decide whether a function is a security function to be evaluated?
  - How to determine appropriateness and completeness of SFR?
  - How to ensure compatibility of PP for the components in an IT system?
    E. g. German eHealth care project: 11 PPs for server, terminals, smart cards

Resistance against attacks

Which level of EAL and resistance to be claimed in PP/ST



Resistance against attacks
Understanding of resistance

How to determine the necessary resistance to attacks in terms of generic levels?

- Consider value of the **assets to protect**
  - Example: PP PC client specific TPM
    → what is the value of the cryptographic key in CC terms of attack potential?
  - Example: PP Point of interaction (electronic cash terminal)
    The PCI scheme measures the values of data and effort of attacks in money.
    → PIN at smart card interfaces >14 - 16k$; PIN >25k$; keys >35k$
- Consider the **threat environment**
  - Example: PP PC client specific TPM
    Is there any key in the TPM, which is secret for the end-user?
    → Specific attack potential quotation tables shall be used for physical attacks
    → Analyze attack potential of physical attacks relevant for the TPM
  - Example: PP Security IC
    Smart cards in the lab of the attacker → all kinds of physical attacks

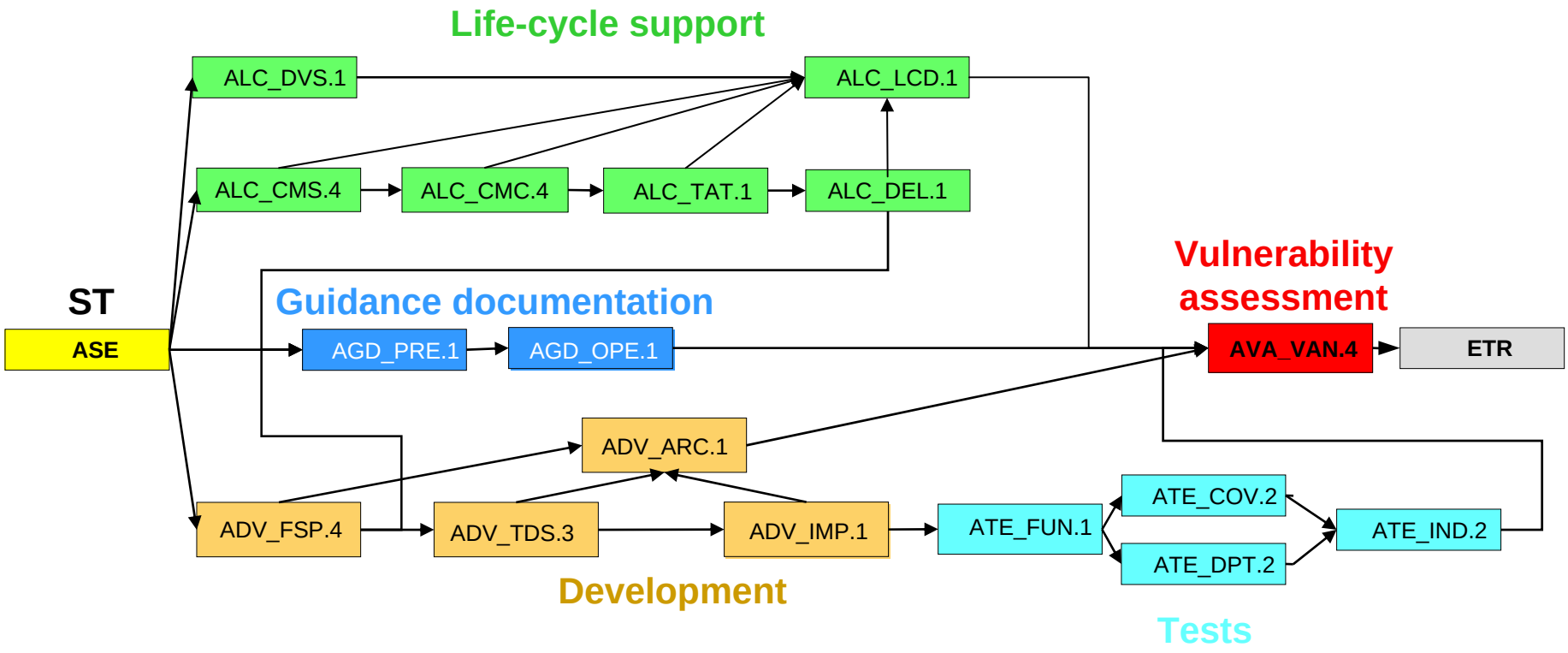
Resistance against attacks

Examples: different resistance for a product

- Machine readable traveller document (MRTD)
  - Personal data of the document holder: enhanced-basic
  - Biometric data of the document holder (fingerprint, iris scan): high
- eHealth server (eHealth connector)
  - Protection of local medical data: enhanced-basic
  - Signature application for qualified electronic signature: high
  - Encryption of medical data: high
- Point of interaction (terminal for credit cards)
  - transaction data: basic
  - card holder PIN: moderate
  - cryptographic key: high

Resistance against attacks

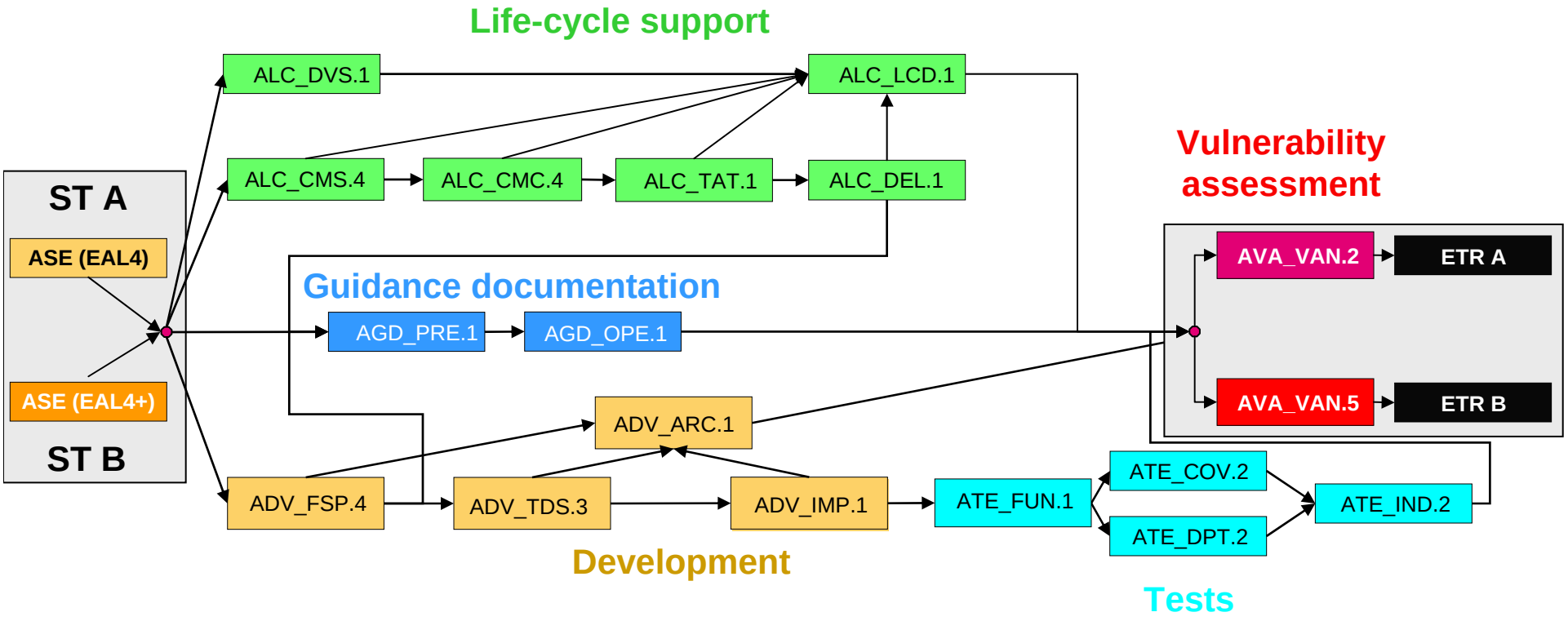
Evaluation workflow of homogenous TOE



Resistance against attacks

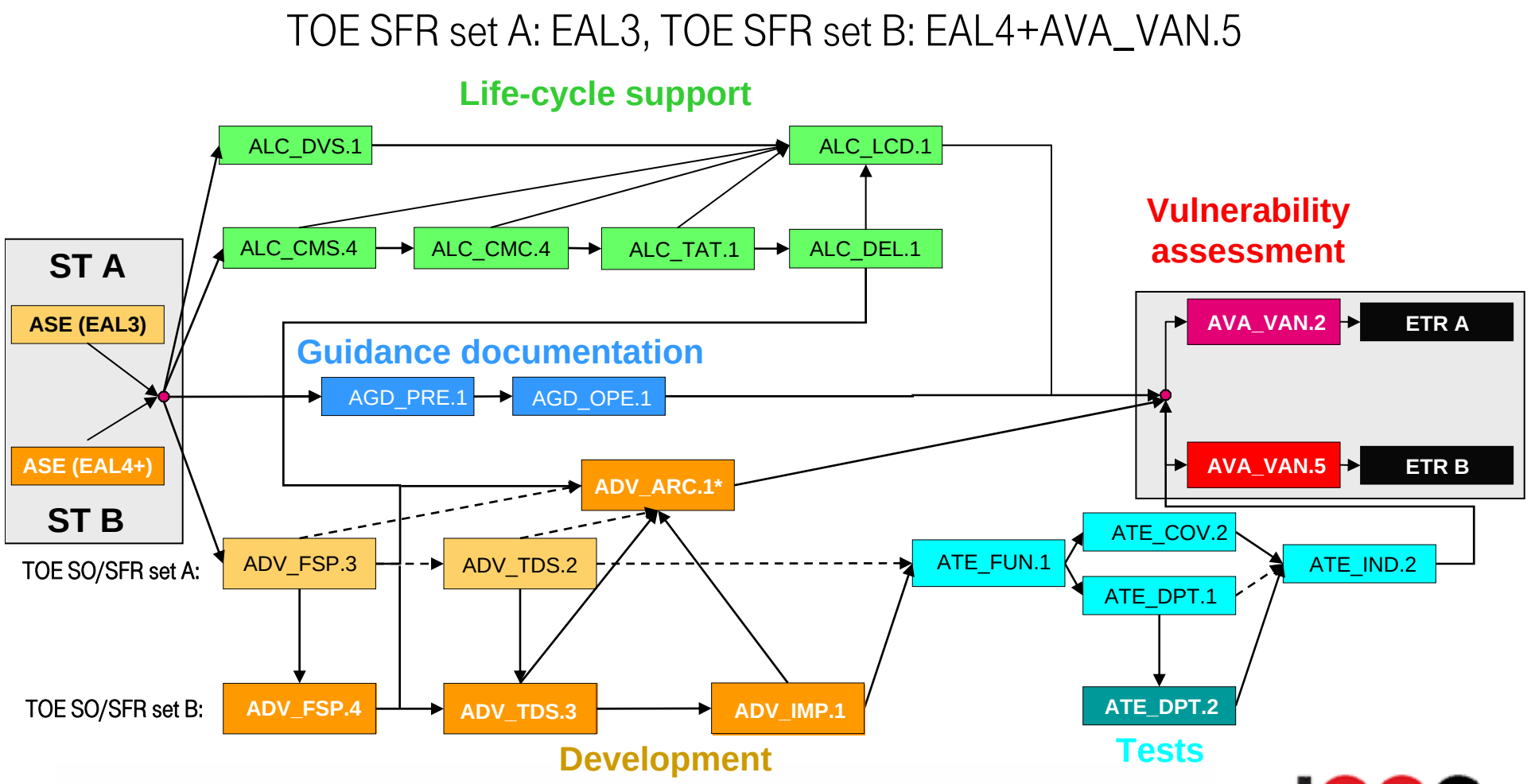
Suggested solution: mainly same EAL, different resistance

TOE SFR set A: EAL4, TOE SFR set B: EAL4+AVA_VAN.5



Resistance against attacks

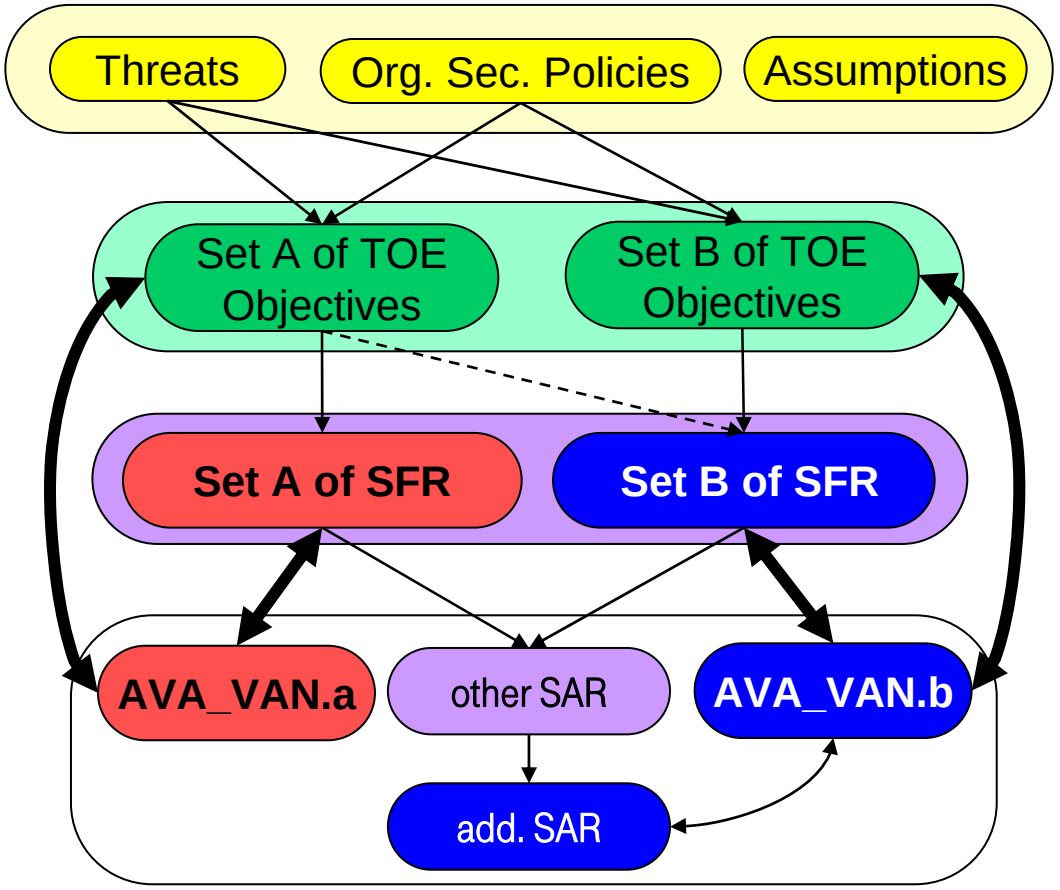
Suggested solution: different EAL and resistance



Resistance against attacks

Suggestion for a future CC version

- A future version of CC may allow for PP and ST with different resistance claims
- AVA_VAN components are linked to
  - non-overlapping sets of security objectives for TOE
  - non-overlapping sets of SFR
  - dependencies of the AVA_VAN components shall be solved by sets of SAR
- Sets of SARs will be applied for the TSF parts implementing the relevant SFR



Conclusion

- PPs are successfully widely used for a huge number of TOE types.
- The intention of the PP issuer is transferred to the product evaluation through the conformance claim. The conformance claim framework of CC should be improved for practical usage.
  Suggestion are made for appropriate changes.
- Definition of security objectives, SFR and SAR, especially AVA_VAN component(s), are crucial for the PP, the ST and the whole evaluation process.
- In order to chose appropriate AVA_VAN component the PP issuer shall have a clear understanding of the value of the assets, the threat environment and the CC attack potential quotation for the TOE product type.
- The TOE may provide different resistance against attacks for different assets. The evaluation should base on 2 ST and result in 2 certificates. Future CC versions might allow for 1 ST, 1 evaluation and 1 certificate.

Thank you for your attention.
Any question?

Wolfgang Killmann
T-Systems GEI GmbH
D-5311 Bonn, Rabinstrasse 8
wolfgang.killmann@t-systems.com