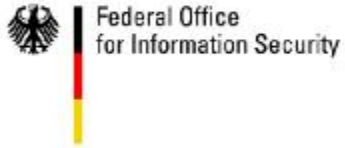
Challenging the concept of one EAL per evaluation



The Trust Provider

TÜViT

Content

- What is it all about?
- Retrospect: The ICCC 2007
  - Problem statement: Why should one EAL not be sufficient?
  - Example
  - Possible solutions today
  - The “Depth of function” approach
- Update: What happened over the last year and where to go
  - Point of Interaction Protection Profile
  - CCCDB
  - CC 4.0

What is it all about?

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

(CC V 3.1 Part I, chapter 1)

- It‘s all about confidence!
- And all about the customer!

Retrospect: ICCC 2007

- For the German e-health system several components are defined in Protection Profiles
- Some of the components live in a conflict of the assurance requirements (as required by the Signature Act) and their functionality
- The Signature Act requires (for relevant components) a certain Evaluation Assurance Level
- The specification of those components requires a certain functionality
- But why should this be a problem? Isn't this just a well defined basis for a Protection Profile?

The e-health terminal PP

- Serves as a secure PIN entry device in accordance with the German Signature Act
  - "The PIN must never leave the terminal in clear text"
  - Has to be evaluated using EAL 3 augmented by AVA_VLA.4 and AVA_MSU.3 (CC 2.3)
- The e-health terminal brings additional functionality compared to classical PIN entry devices:
  - Network connectivity
  - Cryptographic identity
  - Necessary management functionality
- The PP inherits the high assurance requirements from the Signature Act and applies it to the extended functionality
- The requirements from the Signature Act were never meant to be applied to such a complex terminal
- In the end this situation makes evaluations for e-health terminals unnecessary complex

Possible solutions (2007)

- Buy the overhead and include all mechanisms on the high EAL:
  - Overhead in evaluation
  - Overhead in development
  - Total cost will rise
- Exclude non core mechanisms from evaluation:
  - No confidence on excluded mechanisms
- Have two evaluations:
  - Formal overhead
  - Two certificates
  - „Confusing“ for customers

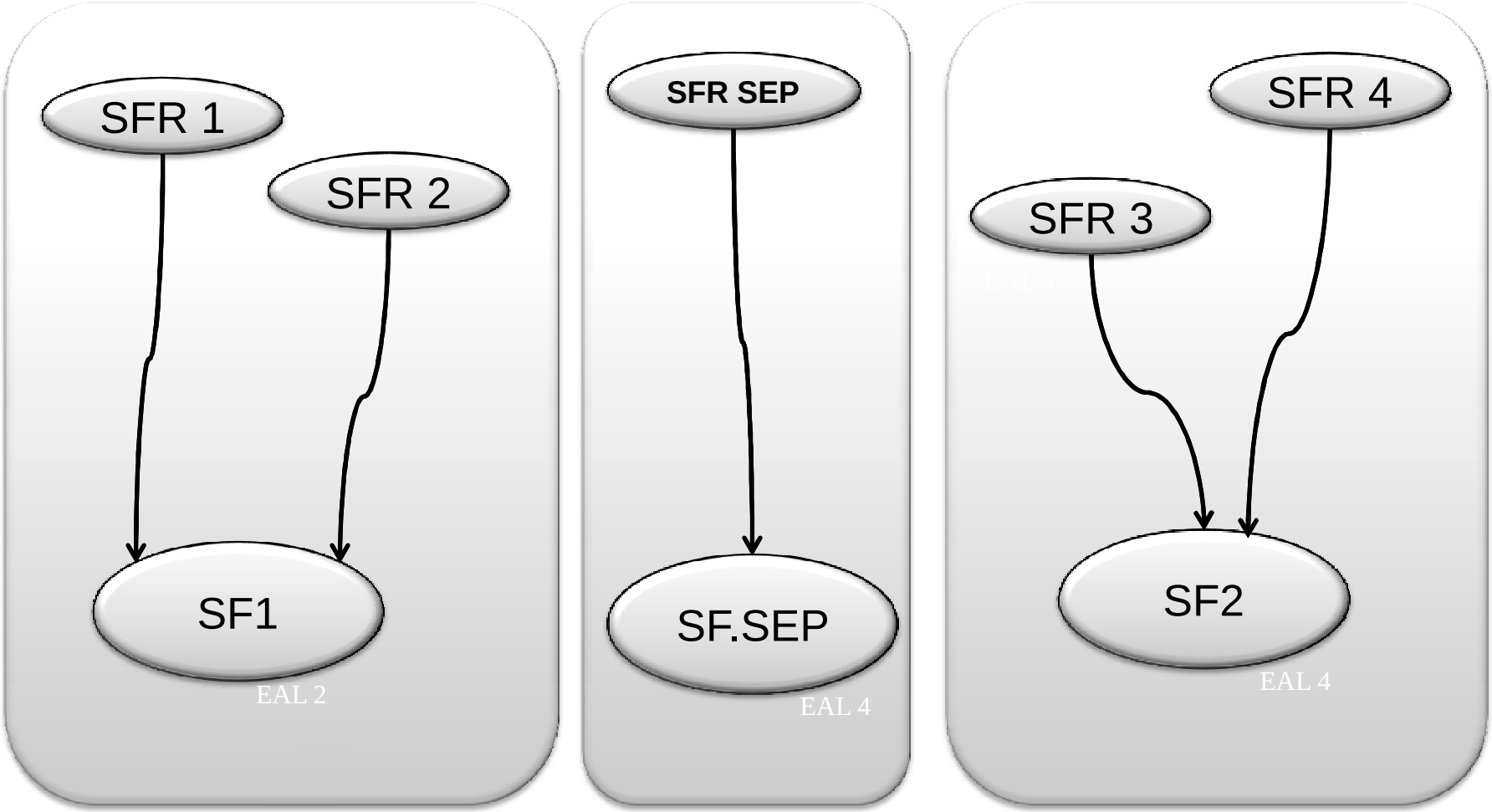
Core questions

- Why should evaluations be limited to one EAL per evaluation?
- More than one EAL per evaluation would make the criteria more flexible
- Customers could require more confidence for one security mechanism than for others
- It would allow evaluations being compliant to more than one set of external requirements; specifically when functional and assurance requirements come from different sources
- This could also be a motivation for developers and customers to specify more security functions in a Security Target than they do today

One EAL per SFR

- One EAL per SFR would be implementation independent and could be specified in a PP
- SFR were introduced to make evaluations comparable and the EAL should be comparable as well
- For SFRs in a PP the mutual support and internal consistency has to be verified. This part of the rationale can be re-used
- SFRs represent a functional unit and are predestinated to serve for linking assurance to functionality
- Mutual support and internal consistency of functionality becomes more important
- An analysis of the implementation of the Security Functions with respect to the EAL becomes necessary.
- Separation of Security Functions becomes very important
- The mechanism for separation of two Security Functions on different EALs has to follow the higher EAL
- Depending on the concrete realization there may not be a need for big structural changes in the criteria

The “Depth of Function” (for CC 2.3)



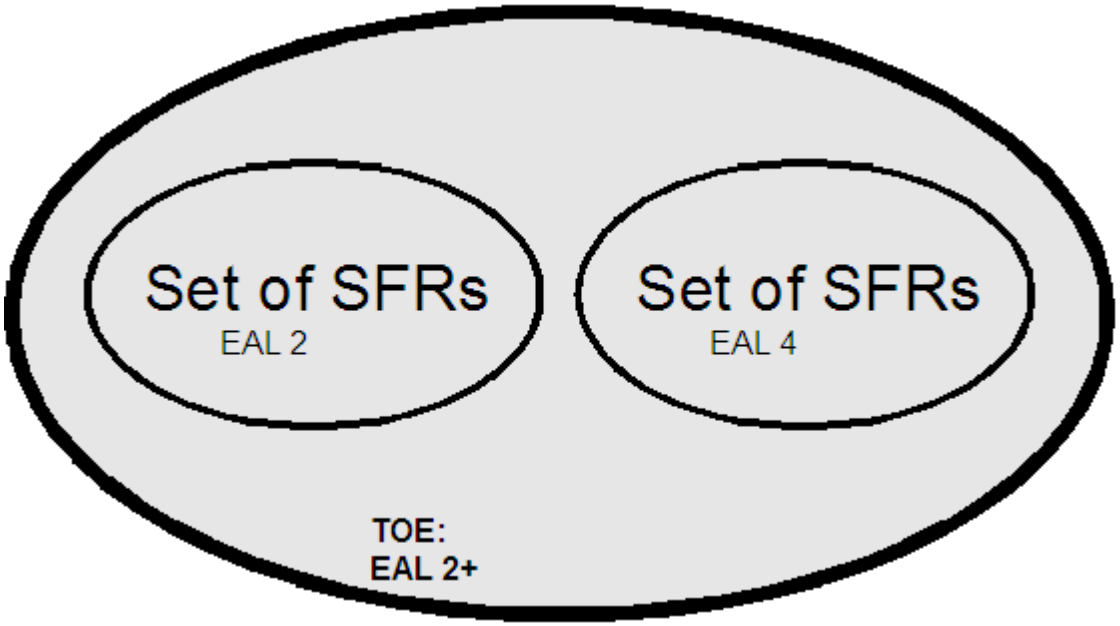
New approach for a PP for payment transactions

- Project established to develop a PP for payment transactions
- The Protection Profile defines the requirements around a TOE that can be used for payment transactions
- Requirement: time- and cost saving approach providing assurance for specific parts of the product comparable to a PCI-evaluation
- The Protection Profile is currently under development
- The project is driven by Germany, Netherlands, France and UK
- Goal of the Project:
  - Providing the evaluator a structured set of developer evidence to gain a better understanding of the product.
  - This should make the vulnerability analysis more effective

One EAL per set of SFRs

- Multiple evaluations for different parts of a product (as exercised e.g. within the German Healthcare System) was rejected
- The PP uses refinements of SFRs to specify the functionality to be evaluated at different assurance levels
- The Approach:
  - SFRs are taken from part 2 or defined according to the CC, including the refinements to separate the different sets of functionality (resp. SFRs)
  - The SFRs are grouped into sets to allow a clear separation of functionality
  - SARs are taken from part 3, including the refinements (alternatively iterations)
  - SARs are clearly mapped to the corresponding part of the TOE and the belonging SFRs
- The concept has not been practically applied during evaluations of the German scheme but is currenlty discussed with different national Certification Bodies

The approach of grouping SFRs for different levels of assurance



Challenges of the new approach

- CC/CEM must partly be interpreted and potentially extended:
  - For each refinement the guidelines of the CEM for the corresponding EAL must be applied, not only the ones for the lowest EAL
  - Scope of additional guidance seems to be limited
- CEM may be „glued“ together by special guidance on evaluation:
  - Specifies how to deal with different requirements on e.g. documentation or testing effort
  - Determines how to deal with ambiguities or conflicts
  - Controls how to document the intersection of the parts evaluated at various depths
- Estimation of costs for an evaluation: evaluation costs will be near those of an evaluation at higher EAL
- The certification of the overall product is „only“ issued on the lower level (augmented) and does not reflect the assurance completely

Summary and Outlook

- In most evaluations today one EAL is sufficient
- In some evaluations multiple EAL can make sense
- Introducing multiple EAL per evaluation would not require a complete rework of the existing criteria
- The work around the Protection Profile for a Point of Interaction showed that
  - There are situations where more than one EAL per evaluation is beneficial
  - Having more than one EAL in an evaluation is feasible
  - The necessary interpretation and guidance for evaluation is not too complex
  - Grouping SFRs and applying one EAL to a group of SFRs is useful
- However, the Protection Profile only defines a “workaround”
- The integration to the existing criteria still needs to be done

Thanks for your attention!

TÜV Informationstechnik GmbH

Member of TÜV NORD Group

Nils Tekampe
Consultant Information Security

Langemarckstr. 20
D-45141 Essen

Phone: +49 201 8999 – 622
Fax: +49 201 8999 – 666
E-Mail: n.tekampe@tuvit.de
URL: www.tuvit.net

Federal Office for Information Security

Miriam Serowy

Federal Office
for Information Security

Godesberger Allee 185 – 189
53175 Bonn

Phone: +49 (0)228 99 9582 5914
Fax: +49 (0)228 99 10 9582 5914
E-Mail: miriam.serowy@bsi.bund.de
URL: www.bsi.de