



REPLACES: N6564

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

- DOC. TYPE:** national body contribution
- TITLE:** German National Body contribution to Common Criteria v.4 regarding multiple assurance level per evaluation
- SOURCE:** DIN, National Body of Germany
- DATE:** 2008-06-25
- PROJECT:** 15408
- STATUS:** In accordance with resolution 5 (see SC 27 N6640) of the 36th SC 27/WG 3 meeting held in Kyoto (April 2008) this document is being circulated to the National Bodies and liaison organizations for for study and comments.
- Submissions should reach the SC 27 secretariat by as soon as possible but no later than 2008-09-05
- DISTRIBUTION:** P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenber, WG-Conveners
- ACTION ID:** **COM**
- DUE DATE:** **2008-09-05**
- MEDIUM:** Livelink-server
- NO. OF PAGES:** 1 + 5

MULTIPLE ASSURANCE LEVEL PER EVALUATION

NILS TEKAMPE, TÜV INFORMATIONSTECHNIK
(N.TEKAMPE@TUVIT.DE)

ABSTRACT

It is one (not to say the) major objective of evaluation according to Common Criteria to provide confidence that the security mechanisms of a product are implemented correctly. The degree of confidence gained by an evaluation can be controlled via the Evaluation Assurance Level (EAL). However, there is only one EAL per evaluation. Thus, currently, it is not possible to gain a high confidence in critical security mechanisms and a lower confidence in other security mechanisms of the same product (during one evaluation), even if the two kinds of mechanisms do not interact.

One example for a project where this has been relevant is the Protection Profile for the German health card terminal. This PP inherits assurance requirements from the German Signature Ordinance and extended functional requirements from the e-health system. The assurance requirements, EAL3 + AVA_VLA.4 and AVA_MSU.3¹, are required by the German Signature Ordinance (with respect to version 2.3 of CC) and usually applied to terminals with a very limited set of functionality. However, based on the current CC assurance principle, these assurance requirements must now be applied to all functionality of the terminal though EAL 2 was the desired EAL for the functionality that was not related to digital signatures. This makes an evaluation according to the PP complex and expensive and requires more sophisticated security mechanisms for the terminal.

In cases such as these, customers and PP authors must decide to accept the overhead of the higher EAL for all mechanisms, reduce the EAL for all mechanisms or exclude non-core mechanisms from evaluation. This paper aims to inspire that – under certain circumstances – it can be useful to have more than one EAL per evaluation.

¹ The required augmentations refer to version 2.3 of Common Criteria. For version 3.1 this will (most likely) result into EAL 3 augmented by AVA_VAN.5, ALC_TAT.1, ADV_TDS.3, ADV_IMP.1 and ADV_FSP.4. However, the rest of the paper will refer to the augmentations for CC version 2.3 as the augmentations for version 3.1 are still under discussion.

SITUATION TODAY

Today the German Signature Act (the Signature Ordinance to be more precise) requires that components in the area of digital signatures are evaluated according to Common Criteria. Functional and assurance requirements are defined for the several components that are involved in creating digital signatures. In this context a smart card terminal that is used as a secure PIN entry device has to be evaluated using EAL 3 augmented by AVA_VLA.4 and AVA_MSU.3. The main scope of the evaluation (from a functional perspective) is hereby to show that the PIN will only be sent to the signature card and cannot be abused.

As part of the German Health Card project Protection Profiles are produced to describe the security and assurance requirements for the core components within the health card infrastructure. As digital signatures are an important aspect for the German e-health system the Signature Act needs to be taken into consideration.

One PP in this context addresses the terminal for the health (professional) card. This terminal can be seen as an extended version of a classical terminal for digital signatures. It serves as a secure PIN entry device but implements additional functionality such as network connectivity, cryptography and extended management functionality. However – as the health professional card is used to generate digital signatures - this terminal has to be compliant with the German Signature Act.

PROBLEM STATEMENT

During the very first steps of the development of the Protection Profile the appropriate assurance level for the extended functionality of the terminal has been discussed and the result has been that a basic assurance (i.e. EAL 2 or EAL 3) would be sufficient considering the role of the terminal in the context of the complete infrastructure that is necessary for the operation of the German Health Card.

However, as the terminal is involved in generating Digital Signatures the Signature Act requires an evaluation on EAL 3 augmented by AVA_VLA.4 and AVA_MSU.3. These assurance requirements that are required by the German Signature Act were never meant to be applied to a terminal with such a complex functionality. Those requirements are referenced to be applied to a terminal that provides one main Security Function: The handling of the user PIN.

As Common Criteria knows only one assurance level per evaluation the Protection Profile lives in a conflict of the fairly high assurance requirements that are required by the German Signature Act and the extended functionality that is required for a smart card terminal to be used within the scope of the German health card.

SOLUTIONS TODAY

As there is only one assurance level per evaluation the following three solutions have been discussed:

- Produce 2 Protection Profiles for one product; one PP for the secure PIN entry device (using EAL 3+) and one PP for the extended functionality of the e-health terminal (using EAL 2 or 3 flat). The disadvantages of this solution are obvious: An enormous overhead in evaluation and two certificates for one product
- A "Threat Model" in the Protection Profile that "ignores" parts of the threats resulting in a PP that ignores a part of the functionality. This solution would result in a PP that only addresses the secure PIN entry device. However, in this solution there would be no assurance at all about the extended functionality of the terminal
- Buy the formal and technical overhead and have one Protection Profile covering all security relevant functionality and defining the EAL 3+ for the German Signature Act.

Each of those solutions has its own advantages and disadvantages. For this example here it was eventually decided to buy the overhead and evaluate the complete terminal on the higher assurance level.

Beside the fact that it is very hard to justify the overhead that is caused by such an evaluation it should be mentioned that by the time that this discussion took place some of the extended mechanisms of the terminal were not designed to undergo such an evaluation.

Specifically the requirements around the vulnerability assessment lead to extra effort in design and development of the terminal. In the end it has been decided to implement a subset of the cryptographic functionality within a Hardware Security Module as part of the terminal as the hardware that is usually used in the area of a smart card terminals couldn't provide the necessary level of protection.

It should be mentioned that the German e health terminal is only one example for the limits of one Assurance Level per evaluation. Similar situations can be found in other Protection Profiles in the area of the German e-health system, point of sales terminals and some E-Passport projects. Basically this issue is likely to occur in cases where the assurance requirements and the functional requirements of one PP are predefined by different specifications/regulations.

The following paragraphs introduce a possible solution for the problem as identified before.

SUGGESTED SOLUTION

Common Criteria is very flexible when it comes to defining the functionality of a product. It allows developers and/or customers to define exactly the set of functionality that they need. At first glance the same flexibility exists for the assurance requirements that are used during an evaluation:

There is no need to stick with one of the predefined Evaluation Assurance Levels. One is free to augment assurance levels by using assurance components from a higher EAL and one can even choose a set of assurance components completely independent from any assurance level (Though this option is not used very often). Finally - for the cases where a kind of assurance is needed that cannot be modeled by the use of existing assurance components from part III of Common Criteria - one is free to refine existing components or define explicit assurance components.

However as outlined before the flexibility is limited as all assurance requirements that are selected (or defined) for an evaluation are applied to the complete Security Functionality of the product under evaluation.

THE SUGGESTED ASSURANCE APPROACH

It should be possible to have a dedicated assurance claim per SFR. The level of SFRs is independent of any concrete implementation and as such it is possible to require such a dedicated claim in a Protection Profile.

The new approach for assurance should base on the following further principles:

1. By default everything should stay as it is. Without a need to have multiple assurance claims per evaluation there should still be one EAL per evaluation. This would mean that an assurance class that may be developed to implement this approach should not be part of any of the predefined assurance levels.
2. For the case that the author of a ST/PP uses dedicated assurance claims for one or more SFR(s):
 - a. The assurance claim for a SFR will have to be traced down to the Security Functionality of the TOE. This means a functionality that implements a SFR with a dedicated assurance claim will have to inherit the assurance claim and the necessary evidences will have to be provided for it.
 - b. A detailed analysis will have to be provided by the developer to show that the provided assurance measures are suitable to fit the claims
 - c. The design documentation will have to show that functions for which less assurance is defined do not interfere with functions that have higher assurance defined
 - d. It is likely that a Protection Profile that uses multiple assurance claims will have to give detailed requirements on how a TOE may be constructed in order to meet the requirements from the PP.

SUMMARY



This paper showed that a concept of multiple assurance claims within one Common Criteria evaluation seems to be feasible and beneficial for the future of the criteria.

Allowing multiple assurance claims within one evaluation would make the criteria more flexible than they are today. It would help to address cases where requirements for one TOE result from different (legal) requirements or different customers and could help developers and sponsors to keep their evaluations close to the reality of their customers' requirements and their development.

As such multiple assurance claims per evaluation can help to improve the flexibility and usability