Swedish Certification Body for IT Security
Scheme note 18 - Highlighted Requirements on the Security Target

Scheme Note

Decision Date CCB 2020-11-19	Matter ID CR-3048 (CR-2596, CR-1887)	
Decision by (Name/Title) Dag Ströman, Head of CSEC	Scheme Note Number 18	Dnr nnnn
Presentation by Jerry Johansson	Present at the Meeting CCB 2020-11-19	

Schematolkningens innebörd/Scheme Note Statement

Description and References

Purpose

The purpose of this Scheme Note is to clarify some of the requirements of the Common Criteria, and the SP-188 Scheme Crypto Policy, on the Security Target (ST). Also, some expectations on the evaluation report (SER ASE) are explained,

Background

Since the Security Target specifies both which functionality to evaluate (SFRs) and which evaluation activities that will comprise the evaluation (SARs), it is important that the Security Target is unambiguous and consistent.

It is important that the evaluator identifies and requests as many as possible of the necessary changes to the ST before the first evaluation report (SER ASE). This will speed up the certification process and reduce extra certifier work.

Requirements

Clarifications of the Common Criteria and the Common Methodology:

1. The TOE Overview in the ST should summarise the security objectives on the operational environment (secure usage of the TOE) and briefly describe the security features. A few lines is sufficient here.
2. The elements of the TOE model that are used in SFRs (subjects, objects, information, resources, operations, external entities and security attributes) must be presented clearly in the ST.
   a) Subjects are active parts of the TOE that do things with data (objects, information, resources) and with other subjects, such as hardware components and software modules. Subjects should be defined in the TOE Introduction.
   b) Objects are passive parts of the TOE where data is stored, such as files, variables or registers. Objects that are mentioned in the SFRs should be defined in the asset list in the Security Problem Definition part of the ST.
   c) Information is data that is stored in objects and that may flow between subjects, objects, and external entities. Information that is mentioned in SFRs should be defined in the asset list in the Security Problem Definition part of the ST.
   d) Resources are services, interfaces etc. which may be convenient when modelling the TOE. Resources that are mentioned in the SFRs should be defined in the asset list in the Security Problem Definition part of the ST.
   e) Operations are a way to describe what the TOE can do. The Logical Scope of the TOE should define the relevant operations of the TOE.
   f) Security attributes are data associated with subjects, objects, information or resources. Security attributes are used in the SFRs.
   g) External entities are users or IT equipment outside the TOE.

3. The Physical Scope of the TOE should describe what the TOE is, i.e. which hardware parts, firmware modules and software modules are considered parts of the TOE. All other parts and modules belong to the TOE environment. This is a natural place to name and describe subjects used in SFRs.
4. The Logical Scope of the TOE should describe what the TOE does – which constitutes the operations of the TOE – and the security features expressed in the context of performing these operations. For a security product, the TOE logical scope and the security features (i.e. the TSF logical scope) may be identical.
5. The assets relevant for the evaluation should be described in the Security Problem Definition (SPD) section in the ST. The assets that are related to threats should be named and described explicitly. The implicit assets (related to organisational security policies, OSPs) shall be obvious from the wording of the OSPs. Implicit assets used in the SFRs shall be named and described in the SPD. Note that everything that is protected by the TSF is an asset.
6. The description of threats and attackers in the SPD must clearly indicate by which means the different attackers can interact with the TOE and which assets are exposed to each threat.
7. The security problem stated in the ST shall be well-defined, non-trivial, and shall not be misleading considering the TOE type and the TOE description.
8. The security objectives in the ST shall be written in the form of security requirements, not functional requirements. Security requirements are claims to protect the assets defined in the ST. All other requirements on the functionality of TOE are functional and therefore should not be part of the security objectives in an ST.
9. SFRs shall be clearly expressed using the subjects, external entities, objects, information, resources, operations and attributes, required by the respective SFR, and all these shall be defined in the ST.
10. All rationales in the ST shall be presented in a logical and coherent manner and on a suitable level of detail.
11. The level of description shall be the similar throughout the entire ST and should be the on the same level as the SFRs.

Clarifications of CSECs SP-188 Scheme Crypto Policy

12. SP-188 refers to recommended cryptographic primitives, modes schemes and protocols. Using any other cryptographic mechanisms implies that the evaluators have to demonstrate that the chosen security mechanisms are secure. When evaluating cryptographic functionality, each combination of primitive and mode/scheme should be considered, and the intended use (e.g. protocol) kept in mind.
13. SP-188 offers the possibility to place the implementation of cryptographic primitives in the environment, but claiming the corresponding FCS_COP.1 SFRs in the ST. Thus the calls to the cryptographic primitives are included in the TSF, but not their implementation. The implementation placed in the environment may contain the symmetrical modes, and the RSA encryption- and signature schemes, but may not contain cryptographic protocols used and claimed by the TOE. Note that the ST shall state clearly that the implementation of the primitives in question has been placed in the environment in accordance with SP-188 Scheme Crypto Policy.

    Placing the implementation in the environment does not affect the evaluation much, but may resolve formal issues such as when source code is not available (at EAL 4 and above, source code shall be available for all parts of the TOE).