Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Reading guide
Protection profiles as per Art. 30 para. 2 of the Ordinance on Electronic Patient Records

The purpose of a Common Criteria Protection Profile (PP) is to formulate the security requirements on a class of product (including in the software or hardware area). By contrast to product and manufacturer-specific security targets (ST), the PP sets out specifications for the requirements on security products in their specific deployment environment and includes the depth of verification necessary to ensure that they are implemented. The “TOE” in the PP is the “Target of Evaluation” which is used to denote representatives of the product class and to which the formulated security targets have to apply.

This document contains an interpretation aid for a Common Criteria protection profile, which is also to be used for the profile in the identification part.
Standards (Common Criteria, Version 3.1 Revision 4):

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components

All the security targets in the PP are to be verified for the specific TOE. The Common Criteria offer a general framework for describing the security functionality and a set of modules which, when drawing up the structural definition of the protection profile, helps specify the security functionality and the depth of verification for a TOE in so-called assurance classes. The aim is to have a comparably verifiable security functionality for products in an individual product class.

Structure of the Common Criteria Protection Profile

The general structure of the protection profile is governed by the Common Criteria. This present document does not go into formal requirements/sections for guaranteeing comparability of the protection profiles developed. Nor does it go into particular special cases, such as the definition of own classes (“extended components definition”).

TOE Overview / Operational environment

This section serves to draw the line between the TOE and external components and to describe the mode of functioning. The components of the TOE are listed, including, in particular, all the parts that provide a security functionality (a so-called TSF, TOE Security Functionality). The parts supported by the TOE security functionalities may also include channels to be constructed to external components outside the TOE, as well as channels between the TOE components themselves. What is important when considering the security of the TOE is also the planned deployment environment. Various assumptions have to be made regarding this environment for secure operation. The assumptions and requirements on the environment mark out the conditions that have to be defined for secure operation.

For the profile associated with the electronic patient records, mention is made inter alia of the IdP (Identity Provider, usually the issuer of means of identification), the secure channels to the (master) community and the access portal for patient login, together with their interaction and the identification functionality of the IdP for the transfer to the authorisation concept imposed by the master community.

Assets

A description of the assets is necessary when describing the security functionality provided by the TOE. Assets are usually authentication and/or authenticating data, as well as key material arising during operation of the TOE plus user data (such as identification data). The assets are subdivided into TSF data and user data. The protection objectives for assets can include not only confidentiality and integrity, but also availability. TSF data can include the key material for building up the secure channels, which is generated in the TOE.

Assets relating to the means of identification for EPD include the identification data and their representativity of the users.

Security Problem Definition / Security Objectives Rationale

The security problem definition contains the definitions and assumptions underlying the formulation of the security targets.

Assumptions here are those preconditions that have to apply for secure operation of the TOE. Organizational Security Policies (abbreviated to P.) are targets which have to apply from the policy perspective in order to implement and/or run the TOE in accordance with the specifications. By contrast to this, the objectives (abbreviated to O.) are delivered through the TOE security functionalities. Objectives for the Environment (abbreviated to OE.) are additional environmental targets. Threats (abbreviated to T.) are the threats that have to be mitigated through TOE objectives.

The Security Objectives Rationale resolves threats, OSPs and assumptions through objectives and objectives for the environment. Multiple assignments are possible here. The rationale is comprised, on the one hand, of a filled matrix and, on the other hand, of a textual description, stating reasons.

The items formulated in connection with the Ordinance on electronic patient records have included the correct handling of credentials by patients and healthcare professionals and also the prior issue of the token as per ISO/IEC 29115:2013. This would have to be ensured as a precondition in the verification.

The threats identified in the context of electronic patient records include, in particular, threats relating to IdP operation. These could be attacks on availability via the visible interfaces (web service and portal) and also, for instance, the appearance of non-trustworthy devices (rogue devices) in the infrastructure.

Security Requirements / Security Requirements Rationale

The Common Criteria describe so-called SFRs (security functional requirements). This is the translation into a standardised normative language of the objective defined for the TOE’s deployment spectrum in the security problem definition (see above). In this connection, the Common Criteria offer the possibility of selecting SFRs from various areas (classes), including “Class FAU: Security Audit” (creation and evaluation of a logfile) or “Class FIA: Identification and Authentication” (identification requirements and the time of authentication of other TOE functions). The SFRs exist with various requirement depths and correlate with each other in some cases. These correlations must always be resolved for a meaningful description. The general structure of each individual SFR offers a description of the requirement that can be aligned to the security functionality of the TOE – in respect of attributes, subjects and objects, and information types, for example.

In the security requirements rationale, the SFRs depict the coverage of the objectives formulated for the TOE (which are to be furnished by the TOE).

Security Assurance Requirements Rationale and Verification of the TOE

The Common Criteria formulate so-called assurance packages, namely evaluation assurance levels (EAL). These apply to the so-called assurance classes of development, guidance documents, life cycle support, security target evaluation, tests and vulnerability, which define the intensity of testing for a TOE. The evaluation assurance levels are already resolved in themselves (for example: testing the functional specification in accordance with assurance class ADV_FSP.2 necessitates testing the design as per ADV_TDS.1. at EAL2). The assurance classes provide sufficient guidance on testing the designs and implementing the TOE in the SFRs described.

For testing the TOE, the instructions for the various assurance classes must be carried out, ensuring compliance with the requirements defined for the TOE’s environment.

The corresponding documentary evidence is captured and verified in a certification process to this end.