SEALWeb

Primekey's EJBCA Enterprise CC evaluation

This note is based on version 3.1, revision 5 of the *Common Criteria for Information Technology Security Evaluation* (so-called "Common Criteria", or "CC") and the *Protection Profile for Certification Authorities* (PP4CA), version 2.1 (National Information Assurance Partnership (NIAP)).

1 DIFFERENCE BETWEEN EAL-PP APPROACH AND CPP

1.1 PRELIMINARY NOTE REGARDING *COMMON CRITERIA*

The reader should be acquainted with the following technical concepts.

The *Common Criteria (CC)* is both a standard and a methodology aiming to allow "comparability between the results of independent security evaluations". The CC does so by providing a common set of requirements for the security functionality of IT products ("security functional requirements", SFR) and for assurance measures applied to these IT products during a security evaluation ("security assurance requirements", SAR). 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 *Common Criteria Recognition Arrangement (CCRA)* allows vendors of a certified products (that its, a product which has been evaluated, in a given country by a given laboratory, and certified to be conformant to some set of SFR's and SAR's) to be recognized in all CCRA nations.

Evaluation Assurance Levels (EAL's) are specified in CC Part 3; they define the predefined CC scale for rating assurance for TOE's. Each EAL consists of some consistent combination of SAR's from CC Part 3:

> *The CC philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon:*
> *a) scope – that is, the effort is greater because a larger portion of the IT product is included;*
> *b) depth – that is, the effort is greater because it is deployed to a finer level of design and implementation detail;*
> *c) rigour – that is, the effort is greater because it is applied in a more structured, formal manner.*

EAL's are thus cumulative, in the sense that all SAR's contained in EAL "n" are either included or augmented (higher level) in EAL "n+1".

1.2 COLLABORATIVE PROTECTION PROFILES AND EAL'S

A *Protection Profile (PP)* is a statement of security requirements for a specific technology. Historically, governments have published their own PP's and vendors needed to comply with each different governmental PP for a given technology. *Collaborative Protection Profiles (cPP)*, on the other hand, have been created by Technical Communities made up of CC and technology area experts with sponsorship from two or more CCRA nations, with the intention to address the heterogeneity of governments' specific PP's whilst defining better requirements and testing methodology through industry engagement.

Hence, collaborative PP's are nothing but standard and CC-compliant PP's. Apart from their redaction process, the other distinctive feature of a cPP is that a cPP does not usually specify an EAL, because cPP's focus on adequate *functional* requirements (SFR's) for a given product/technology. Here, the relevant distinction that must be understood is that a PP's SFR's describe the security functionalities of a product, while the SAR's define the "level of effort" (CC Part 3, §6.3) required during the evaluation process. Adequacy of a product to a given field/function is hence actually contained in the PP's SFR's, not by the (optional) SAR's.

2 THE COLLABORATIVE PROTECTION PROFILE FOR CERTIFICATION AUTHORITIES, WHAT'S INSIDE ?

The collaborative Protection Profile for Certification Authorities "is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats". It contains 78 SFR's and all the elementary assurance requirements of the EAL1 package.

The PP4CA abundently uses the so-called "extended components" of the CC: requirements in an ST or a PP are not necessarily based on components from CC Part 2 or CC Part 3 and can be defined by the ST/PP authors, as long as they are "clear, unambiguous and evaluatable" (CC Part 1, section C.4) ; such requirements are called "Extended components". About two thirds of the PP4CA's SFR's are extended, and the extensions are used to (1) specialize the standard CC SFR's to the PKI domain (for instance, *Identification and Authentication* (FIA) components are extended to accurately reflect the X.509 certificate validation procedures) and (2) specify assurance activity for these components (what must be done during the CC evaluation of the TOE).

For instance, the capability to generate certificates using profiles that comply with requirements as specified in IETF RFC 5280 is expressed in the extended component "FDP_CER_EXT.1", certificate status information, as expressed in §6.3.10 of ETSI EN 319411-1 is provided in the extended component "FDP_CSI_EXT.1", and so on. Readers acquainted with ETSI EN 319411 and ETSI EN 319401 will recognize the usual requirements on PKI management and operation: media handling as in §7.3.2 of ETSI EN 319401 (FDP_RIP.1), rules for certificate validation (FIA_X509_EXT.1 and FIA_X509_EXT.2), trusted roles defined in REQ-7.2-15 of ETSI EN 319401 (FMT_SMR.2), trusted/controlled software update, as REQ-7.7-09 of ETSI EN 319401 (FPT_TUD_EXT.1), forbiddance of plaintext key export (FPT_KST_EXT.1), key protection (FPT_KST_EXT.1 and FPT_KST_EXT.2), *etc.*[1]

In these extended components, **the added assurance activities augment the assurance requirements beyond those of EAL1** that are included in the PP4CA. These assurance activities also ensure that these extended SFR's are "evaluatable". For instance, Assurance Activity of FAU_GEN.1 states that:

[1] For the sake of completeness, we note that authentication mechanism in FIA_UAU_EXT.1 is weaker than GEN-6.5.5-04 in ETSI EN 319411-1.

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed […]

This should include all instances of an event. […]

The evaluator shall ensure the audit records generated during testing match the format specified in the operational guidance, and that the fields in each audit record have the proper entries and that the audit records are provided in a manner suitable for interpretation. The evaluator shall also ensure the ability to apply searches of audit data based on the type of event, the user responsible for causing the event, and identity of the applicable certificate.

Such activity can be considered to be a focused version of the SAR "ATE_IND.2" ("Independent testing", which is included in EAL's up to EAL6), one where the evaluator tests the TOE, not according to the "developer tests" (as in ATE_IND.2), but to his own set of functional tests, which must cover the described functional perimeter. Note that this perimeter actually covers all the extended SFR's, as every Assurance Activity includes a "Test" activity.

Similarly, several test assurance activities can be considered equivalent to the "AVA_VAN.2.3E" actions[2], where the evaluator attempts to circumvent the TOE's security functions by performing "attacks [as an] attacker possessing Basic attack potential" ; for instance:

(from FDP_CER_EXT.3) Test 3: The evaluator shall attempt to construct one or more certificate requests that violate the rules for automatic approval, and shall verify that the requested certificates are not issued.

3 PRIMEKEY'S EJBCA ENTERPRISE CC EVALUATION

First, one should note that PKI core software is not the target of high-level attackers: such software is not directly exposed on the Internet, and environmental protection measures are assumed to exist (firewalls, IDS, etc.). Second, the CA's critical assets are the Cryptographic keys, which are protected by another, physical, component (HSM); this is why ETSI standards do not require PKI software to be certified. Nevertheless, the CC-evaluation of the software is a

[2] (from AVA_VAN.2) The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

very good practice to bring more confidence in the robustness of the CA's IT environment and the security of the HSM's IT clients.

Because PP4CA's default EAL level is 1, one could be – erroneously – tempted to conclude that conformance to that cPP only provides "some confidence in correct operation" and that "threats to security are not viewed as serious" (as expressed by the CC for EAL1's applicability). Indeed, as noted in the previous sections, PP4CA contains far more assurance requirements than the sole EAL1 SAR's: both extended and standard SFR's include additional detailed Assurance Activity requirements which augment the actual assurance level of the PP.

The extended SFR's make this cPP a very accurate protection profile for the core PKI components of a CA; moreover, the detailed assurance activities allow the evaluators to consistently and adequately perform the required evaluation tasks in a more efficient way than, for instance, a generic EAL3 evaluation, because the precise test instructions focus on the domain-specific aspects of the security functions.

In brief, CC-evaluation of a PKI software with respect to the PP4CA is an efficient way to obtain a well-founded assurance that the said software actively contributes to the security of the CA's HSM's IT security environment and to the conformance of the CA's organisation and practices to the ETSI EN 319411/319401 standards.

SEALWeb contact: