Common Criteria Recognition Arrangement
Management Committee

Operating Procedures

Document Number: 2017-01-23

Version: 1.0 draft 0.5
Date: January, 2017

Subject: Certificate validity.

Problem definition

Common Criteria certificates generally have indefinite validity period unless they are withdrawn. Yet, there is no way for a common user, procurer, or legislator to appreciate if a certified product is suitable for use, especially for continuous use, in a specific context.
Indeed both the intended environment of use and the attackers' know-how may change over time, possibly making a certified product unsuitable for use. In particular, when the attack environment has changed over time, risk managers and approval bodies need to be able to estimate the appropriateness of a product in this new environment.
This note provides details regarding CC certificate validity for risk management and conformance approval bodies and also presents several processes allowing to manage this validity.

Certificate validity

Certificate technical validity

A certificate states the assurance level claimed by the product in the security target is reached at the time it is issued. As the attack method evolves over time, the resistance of the product to new attacks is no more covered by the certificate. Thus certificates can only be considered technically valid at their time of issuance.
Indeed, since it is not known at the time of issuance how the attack method will evolve, there can be no time period associated to the technical validity of a certificate.

Certificate administrative validity

Nevertheless, a certificate should come with a definite validity period. As stated before, validity here is not to be understood as technical validity, i.e. linked to the resistance of the product to attacks, but as administrative validity. It should only allow evaluation sponsors to communicate on their certification investment. By default a lifespan of 5 years seems to be a good balance between certification body requirements and business requirements. This default lifespan may be refined at CCDB level for specific PPs.
At the end of this period the certificate shall be archived. Archived certificates can no more be considered administratively valid.

Administrative validity should be clearly identified for all certificates.
It should be noted that the availability of a certificate in the certification list does not guarantee that the related product is itself available to potential customers.

Surveillance/reassessment

This process allows to establish long-term technical trust in certified products, or more precisely trust in their resistance to attackers, taking into account state-of-the-art developments in the field of attacks. This process can only be applied if the product hasn't changed since its initial certification.
Surveillance/reassessment consists in periodical or ad-hoc updates of the vulnerability analysis of the initially certified product, at the same level as initially requested within the security target, including when necessary the associated penetration tests. Only an evaluation facility with a good knowledge of the product can be a candidate to do the surveillance/reassessment of this given product (typically, the evaluation facility that has carried out the initial evaluation of the product). The surveillance/reassessment results in a report established by the CB. If the initial certificate was subject to mutual recognition, the surveillance/reassessment report will have to be public.
The period of Surveillance/reassessment has to be defined by the sponsor according to their customers need.
If the initial AVA_VAN level of the product is confirmed, it is then assumed that the initial certificate is still technically valid.
The administrative validity of the certificate is then extended for 5 years (or the adequate PP specific time period).
As the attack method evolves over time the resistance of the product against new attack method is not covered by the surveillance/reassessment results.

Assurance continuity

According to [CCRA 2012-06-01] (2012-06-01, Assurance Continuity: CCRA Requirements, Version 2.1), the assurance continuity paradigm defines two processes: maintenance and re-evaluation.
When a maintenance report is issued it has no impact nor on the technical validity nor on the administrative validity as no additional tests are made by the ITSEF after the initial evaluation.
When a new certificate is issued (after re-evaluation) both administrative and technical validity can be reset as the latest state of the art attacks have been taken into account during the evaluation process. Note that the reevaluation workload could be reduced regarding the initial evaluation by reusing results of this initial evaluation.