Title: Certificate validity.
Maintained by: CCDB
Unique Identifier: 012
Version: 1.0
Status: Final
Date of issue: 2021-Sep-30
Approved by: CCMC

Problem definition

Common Criteria certificates have in the past been issued with unlimited validity period, unless they are withdrawn. Hence, there was no way for a common user, procurer, or regulator to estimate if a certified product was still suitable for use, especially for continuous use, in a specific context.

Indeed, both the intended environment of use and the attackers' know-how may evolve over time, possibly making a certified product unsuitable for use. It is though of particular importance, especially when the threat environment has evolved over time, that risk managers and approval bodies are able to estimate the appropriateness of a product in this new environment.

CCDB has approved a resolution, effective 1 June 2019, to limit the validity of mutually recognized CC certificates over time.

This document provides information for vendors, risk managers and approval bodies on CC certificates validity. It also defines the minimum requirements to be implemented by CCRA member nations regarding the validity of CCRA recognized certificates. It does not preclude such nations from having further requirements in their implementation of Certificate Validity.

Certificate validity

A certificate states the assurance level reached by a product at the time it is issued. As the threat environment evolves over time, the resistance of the product to new attacks is not captured anymore by the certificate. In other words, certificates can only be considered technically valid at their time of issuance. Indeed, because the evolution of the state-of-the-art regarding attack methods cannot be predicted, there can be no time period associated to the technical validity of a certificate. It is the responsibility of users and risk owners to have a risk management process in place to decide on the use of a certified product and its operational environment.

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. Administrative validity is related to administrative tasks such as advertising of certificates on a CPL and archiving of evaluation evidence. A default lifespan of 5 years has been considered a good balance between certification bodies requirements and business requirements. This default lifespan may be refined at CCDB level for specific PPs.

Certificate archiving

Following the resolution by the CCRA to define a default validity period, certificates will be displayed no more than five years (or the corresponding specific period defined by the CCRA for any particular PP) on the Certified Products List, unless their validity has been extended.
After their validity has expired, certificates will be moved to the 'Archived Certified Products' list.
Archived certificates can no more be considered valid.
It should however be noted that the reference of a certificate in the Certified Products List or the Archived Certified Products List does not say anything about the availability of the related product itself to potential new customers.

Assurance continuity

The validity of a certificate can be extended using the re-assessment process.
Re-assessment allows establishing updated trust in certified products, more precisely trust in their resistance to attacks, taking into account the latest state-of-the-art developments. Following a positive re-assessment, the validity of a certificate will be extended for a period of 5 years (or the corresponding specific period defined by the CCRA for any particular PP).

Though its principles have been agreed, the details of this process need further work by the CCDB to ensure consistent implementation by CCRA members.
The re-assessment process will be defined in a future update of Assurance Continuity (2012-06-01).

Validity declaration

The validity date shall be printed on the certificate or the certification/validation report (i.e. expiration date: <certification date plus x years>).

The certificate or certification/validation report shall make a reference to this procedure regarding the definition of certificate validity.

The Certified Products List, whether on the CB or the CCRA website, shall clearly state the validity date of certificates.