PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 23 septembre 2021

Référence **: ANSSI-CC-NOTE-25_v1.0EN**

APPLICATION NOTE

SCOPE REDUCTION OF A CC CERTIFICATE

Application **:** From its approval.

Circulation **:** Public

COURTESY TRANSLATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

VERSION HISTORY

Version	Date	Modifications
1	23/09/2021	Creation

This note is also submitted for opinion on each major change in accordance with the Certification Center's quality manual. Minor evolutions are not submitted to the certification management committee.

This instruction is available online at the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1 Subject of the Note

During a certified product's life cycle, new attacks may appear that may impact the security of some of the product's features without affecting others.

To deal with this kind of situation, the classic approach recommended by ANSSI, consists of correcting the product in order to counter the exploited vulnerabilities for these new attacks. A re-evaluation of the product is then necessary in order to verify that the modifications made are effective and are not impacting other product's security features (see [CC-MAI-P-01]).

However such an approach isn't always compatible with the CC evaluation sponsor's cost and time constraints. This application note proposes an approach to reduce the scope of a CC certificate allowing the edition of an update of the certificate at low cost and within a reduced timeline.

2 Scope reduction analysis

The work analysis of the scope reduction focuses on the impact of the scope reduction on the initial evaluation compliance tasks. They allow the analysis of the explicit exclusion of certain product's interfaces or the restriction of the means of access mentioned on the initial certificate.

The scope reduction analysis activities mainly consist of verifying that the exclusion or the restrictions of the access proposed to the interfaces:

- Effectively eliminate the application of new attacks (effectiveness of the scope reduction) ;
- Do not impact other product's features (harmlesness of the scope reduction).

This approach does not allow to update the product's vulnerability analysis results, so it is not a substitute of a CC re-evaluation approach.

2.1 Scope reduction effectiveness

Excluding or restricting the use of an interface allows to eliminate any attack path using that interface. It is therefore necessary to ensure that there is no other attack path enabling the exploitation of the vulnerability related to this new attack through an interface that is still available.

The verdict of the analysis will be « Non conclusive » if:

- The argument provided by the developer is considered too complex for the ITSEF to allow to decide on the basis of a documentary review ;
- The ITSEF exhibits attack paths still applicable despite the scope reduction.

2.2 Scope reduction harmlesness

Some functionalities carried out by the excluded interfaces may be necessary to perform security functionalities still included in the proposed new scope (e.g. exclusion of an interface that performs a necessary authentication to perform a TOE's security policy). It should therefore be verified that other product functionalities do not rely on the excluded interfaces.

In addition, the documentary deliverables consistency shall be ensured: The ITSEF must ensure that the list of modifications announced in the Impact Analysis document allows to maintain the consistency of the evaluation's deliverables and that the resumption of the evaluation's activities will remain reasonable and proportional to those changes.

The verdict of the analysis will be « Non conclusive » if:

- The ITSEF identifies product functionalities that rely on excluded or restricted interfaces;
- The ITSEF identifies inconsistencies among the deliverables

3 Scope reduction analysis steps preview

The scope reduction approach consists in two steps:

- step 1 : analysis of the proposed modifications to determine the feasibility of the scope reduction analysis;
- step 2 : resumption of the documentary evaluation activities impacted by these modifications.

3.1 Step 1

The sponsor provides the ITSEF the following elements:

- A new security target based on the previous one and explicitly indicating the interfaces to be excluded or restricted, as well as the impacts of these deletions and restrictions over the response to the security problem (e.g. removal of a security objective and/or threat related to the excluded functionality);
- Update of the user guides excluding the interfaces in question;
- An Impact Analysis modifications document including the following elements :
    - The list of modifications to be made to the evaluation deliverables;
    - For each modification, an impact analysis on the evaluation activities (in terms of the affected CEM's work units);
    - The attacks that are supposed to be prevented and that are the subject of the modification ;
    - An argument justifying the effectiveness of the restrictions with regard to the attacks in question;
    - An argument justifying the non-impact of the scope reduction over the security functionalities retained in the certification scope ;
    - An exhaustive list of the composite products based on the certificate targeting the scope reduction and the functional impact on these composite certificates.

The ITSEF which conducted the initial product evaluation analyzes these deliverables and issues a verdict on the feasibility of a scope reduction analysis. A scope reduction analysis will be considered "feasible" if the evaluation workload to process the ASE, ADV, AGD, ALC (site audits not taken into account) compliance tasks are significantly lower than those of the initial evaluation. In this case, step 2 is initiated.

The certification center must be notified by email of the start of these activities and its results.

3.2 Step 2

A re-evaluation request is issued to the certification center to describe the scope reduction analysis work which will correspond to classes ASE (including the PP compliance study), ADV, AGD, ALC (sites audit not taken into account) and ATE. This evaluation is treated in accordance to the nominal certification procedure (see [CC-CER-P-01]). The certification center may refuse the application if it considers that the impact of the scope reduction of the certificate on the composite products is not controlled.

The developer forwards the ITSEF and the certification center the modified evaluation deliverables.

The ITSEF evaluates the new deliverables and establishes the verdicts of the reopened evaluation activities in a technical report of scope reduction analysis. This report states the overall evaluation activities, either by justifying that the work previously carried was not impacted by the modifications, or by remaking a part or the complete activities concerned by the new deliverables.

In the case of a platform (as defined in [JIL_COMP]), the composition report will be updated with the scope reduction analysis elements and will reference the new CC document versions delivered by the developer.

4 Certification Report linked to a scope reduction

Once the scope reduction analysis report is approved by the certification center, a certification report and a certificate will be issued with the following particularities:

- The certification report and the certificate correspond to an incremented version of the previously issued report and certificate;
- The certification report clearly establishes that it states over the effectiveness of the modifications to exclude the new attacks identified and that the overall resistance of the product to the state-of-the-art attacks, has not been updated since the initial certification or the latest "surveillance";
- The certification report also clearly establishes that the validity of the site audits has not been updated.

In addition, it is important to highlight that end date of the validity of the corresponding certificate remains the same as the initial certification or "surveillance".

ANNEXE A. References

Reference	Document
[CC]	*Common Criteria for Information Technology Security Evaluation*, version en vigueur.
[CEM]	*Common Methodology for Information Technology Security Evaluation*, version en vigueur.
[CC-CER-P-01]	Certification Critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version en vigueur.
[CC-MAI-P-01]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01
[JIL_COMP]	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version en vigueur.

The majority of these documents can be consulted or downloaded from the ANSSI website (www.ssi.gouv.fr).