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

N° **2387/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-NOTE-25_v1.0**

NOTE D'APPLICATION

REDUCTION DE PORTEE D'UN CERTIFICAT CC

Application **:** Dès son approbation.

Diffusion **:** Publique.

Le sous-directeur « Expertise » de l'Agence nationale de la sécurité des systèmes d'information

Renaud LABELLE
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1	23/09/2021	Création

En application du décret n°2002-535 du 18 avril 2002 modifié, la présente note a été soumise, lors de sa création, au comité directeur de la certification, qui a donné un avis favorable.

Cette note est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évolutions mineures ne sont pas soumises au comité directeur de la certification.

La présente note est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

TABLE DES MATIERES

1 Objet de la note

Au cours de la vie d'un produit certifié de nouvelles attaques qui impactent la sécurité d'une partie des fonctions du produit sans en affecter d'autres peuvent apparaître.

Pour faire face à ce genre de situation, l'approche classique, recommandée par l'ANSSI, consiste à corriger le produit afin de parer aux vulnérabilités exploitées par ces nouvelles attaques. Une réévaluation du produit est alors nécessaire afin de vérifier que les modifications apportées sont efficaces et qu'elles n'impactent pas les autres fonctions de sécurité du produit (voir [CC-MAI-P-01]).

Cependant une telle approche n'est pas toujours compatible avec les contraintes de coût et de délai des commanditaires des évaluations CC. La présente note d'application propose une démarche de réduction de portée d'un certificat CC permettant, à faible coût et dans un délai réduit, l'édition d'une mise jour d'un certificat.

2 Analyse de la réduction de portée demandée

Les travaux d'analyse de la réduction de portée sont centrés sur l'impact de cette réduction de portée sur les tâches de conformité de l'évaluation initiale. Ils permettent l'analyse de l'exclusion explicite de l'accès à certaines interfaces du produit ou de la restriction de leurs modalités d'accès sur le certificat initial.

Les activités d'analyse de la réduction de portée consistent principalement en la vérification que l'exclusion ou la restriction d'accès proposées aux interfaces :

- éliminent effectivement l'application des nouvelles attaques (efficacité de la réduction de portée) ;
- n'impactent pas les autres fonctionnalités du produit (innocuité de la réduction de portée).

Cette démarche ne permet pas la mise à jour des résultats d'analyse de vulnérabilités du produit, elle ne se substitue donc pas à une démarche de réévaluation CC.

2.1 Efficacité de la réduction de portée

L'exclusion ou la restriction d'utilisation d'une interface permet d'écarter tout chemin d'attaque utilisant cette interface. Il convient dès lors de s'assurer qu'il n'existe aucun autre chemin permettant d'exploiter la vulnérabilité liée à cette nouvelle attaque au travers d'une interface toujours disponible.

Le verdict d'analyse sera « Non concluant » si :

- l'argumentaire fourni par le développeur est jugé trop complexe par le CESTI pour lui permettre de statuer sur la base d'une analyse documentaire ;
- le CESTI exhibe des chemins d'attaque toujours applicables malgré la réduction de portée.

2.2 Innocuité de la réduction de portée

Certaines des fonctionnalités portées par les interfaces exclues peuvent être nécessaires à la réalisation de fonctions de sécurité toujours incluses dans la nouvelle portée proposée (par exemple, exclusion d'une interface réalisant une authentification nécessaire pour la réalisation d'une politique de sécurité de la cible). Il convient donc de vérifier que les autres fonctionnalités du produit ne s'appuient pas sur les interfaces exclues.

Par ailleurs, la cohérence des livrables documentaires doit être assurée : le CESTI doit s'assurer que la liste des modifications annoncées dans le document d'analyse d'impact permet de maintenir la cohérence des livrables d'évaluation, et que la reprise des activités d'évaluation restera raisonnable et proportionnelle à ces modifications.

Le verdict d'analyse sera « Non concluant » si :

- le CESTI identifie des fonctionnalités du produit qui s'appuient sur des interfaces exclues ou restreintes ;

- le CESTI identifie des incohérences entre les livrables.

3 Aperçu des étapes d'analyse de la réduction de portée

La démarche d'analyse de la réduction de portée fonctionne en deux étapes :

- étape 1 : analyse des modifications proposées pour déterminer la faisabilité de l'analyse de la réduction de portée ;
- étape 2 : reprise des activités d'évaluation documentaire impactées par ces modifications.

3.1 Etape 1

Le commanditaire fournit au CESTI les éléments suivants :

- une nouvelle cible de sécurité basée sur la précédente, et faisant apparaître de façon explicite les interfaces à exclure ou à restreindre, ainsi que les impacts de ces suppressions et restrictions sur la réponse apportée au problème de sécurité (ex : suppression d'un objectif de sécurité, d'une menace propre à la fonctionnalité exclue, etc.) ;
- la mise à jour des guides d'utilisation excluant les interfaces considérées ;
- un document d'analyse d'impact des modifications incluant les éléments suivants :
    - la liste des modifications à apporter sur les livrables d'évaluation ;
    - pour chaque modification, une analyse des impacts sur les activités d'évaluation (en termes des unités de travail de la CEM impactées) ;
    - les attaques qui sont censées être évitées et qui font l'objet de la modification ;
    - un argumentaire justifiant l'efficacité des restrictions opérées vis-à-vis des attaques considérées.
    - un argumentaire justifiant du non impact de la réduction de portée sur les fonctionnalités de sécurité conservées dans la portée de certification ;
    - la liste exhaustive des produits composites s'appuyant sur le certificat visant la réduction de portée et l'impact fonctionnel de cette réduction de portée sur ces certificats composites.

Le CESTI qui a procédé à l'évaluation initiale du produit analyse ces livrables et émet un verdict sur la faisabilité d'une d'analyse de la réduction de portée. Une analyse de la réduction de portée sera considérée comme faisable si les charges d'évaluation pour traiter les tâches de conformité ASE, ADV, AGD, ALC (hors audits de site) sont significativement inférieures à celles de l'évaluation initiale. Dans ce cas, l'étape 2 est engagée.

Le centre de certification doit être averti par courriel du démarrage de ces activités et de ses résultats.

3.2 Etape 2

Une demande de réévaluation est émise vers le centre de certification pour décrire les travaux d'analyse de la réduction de portée qui correspondra aux classes ASE (dont l'étude de conformité au PP), ADV, AGD, ALC (hors audits de site) et ATE. Cette évaluation est traitée conformément à la procédure nominale de certification (voir [CC-CER-P-01]). Le centre de certification peut refuser la demande s'il juge que l'impact de la réduction de portée du certificat sur les produits composites l'utilisant n'est pas maîtrisé.

Le développeur transmet au CESTI et au centre de certification, les livrables d'évaluation modifiés.

Le CESTI évalue les nouveaux livrables et établit les verdicts des activités d'évaluation réouvertes dans un rapport technique d'analyse de la réduction de portée. Ce dernier statue sur toutes les activités d'évaluation, soit en justifiant que le travail réalisé précédemment n'est pas impacté par ces modifications, soit en refaisant une partie ou l'ensemble des activités concernées par les nouveaux livrables.

Dans le cas d'une plateforme (au sens de [JIL_COMP]), le rapport pour composition sera mis à jour avec les éléments d'analyse de la réduction de portée et référencera les nouvelles versions des documents CC livrés par le développeur.

4 Rapport de certification lié à une réduction de portée

Une fois le rapport technique d'analyse de la réduction de portée approuvé par le centre de certification, un rapport de certification et un certificat sont émis avec les particularités suivantes :

- le rapport de certification et le certificat correspondent à une version incrémentée du rapport et du certificat précédemment émis ;
- le rapport de certification établit clairement qu'il statue sur l'efficacité de la modification pour écarter les nouvelles attaques identifiées et que la résistance globale du produit aux attaques de l'état de l'art n'a pas été mise à jour depuis la certification initiale ou la dernière surveillance ;
- le rapport de certification établit aussi clairement que la validité des audits de site n'est pas mise à jour.

Par ailleurs, il est important de souligner que la date de fin de validité du certificat associé reste celle de la certification initiale ou de la dernière surveillance.

ANNEXE A. Références

Référence	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.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.ssi.gouv.fr).