Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 1er février 2017

N° 560/ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-NOTE-21/1.0

NOTE D'APPLICATION

METHODOLOGIE POUR L'EVALUATION D'UNE GAMME DE PRODUITS

Application : Dès son approbation

Diffusion : Publique

Le directeur général
de l'agence nationale de la sécurité
des systèmes d'information

P/O Vincent STRUBEL
Sous-directeur Expertise
[ORIGINAL SIGNE]

Suivi des modifications

Editions	Date	Modifications
1	01/02/2017	Création

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

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

TABLE DES MATIERES

1. Objet de la procédure

Dans le cadre des évaluations selon les Critères Communs (CC), ou selon la méthodologie de certification de sécurité de premier niveau (CSPN), un développeur ou commanditaire peut être amené à faire évaluer non pas un produit, mais une gamme de produits.

La présente note a pour objectif de préciser les particularités des évaluations CC et CSPN de gammes de produits.

2. Références

- ANSSI-CSPN-CER-P-01 – Procédure de Certification de sécurité de premier niveau des produits des technologies de l'information ;
- ANSSI-CSPN-MAI-P-01 – Maintien de la confiance : continuité de l'assurance.
- ANSSI-CC-CER-P-01 – Procédure de Certification de produits.
- ANSSI-CC-MAI-P-01 – Procédure de continuité de l'assurance.

3. Terminologie

Gamme de produits	Une gamme de produits peut être définie comme un ensemble de produits proposé par un même fabricant, répondant à un besoin de sécurité identique et partageant un socle commun de fonctionnalités, mais qui diffèrent par un certain nombre de caractéristiques (design, hardware, micro-logiciel, logiciel etc.). Ces différences peuvent être liées, par exemple, au matériel ou à la plateforme sous-jacents, ou à des fonctionnalités complémentaires correspondant à des périmètres fonctionnels ou des besoins de performance plus ou moins importants.
Produit de référence	Le produit choisi par le développeur ou commanditaire comme étant représentatif de la gamme. Il correspond à la principale cible des travaux d'évaluation.
Produits déclinés	Tous les produits faisant partie de la « gamme de produits » à l'exception du « produit de référence ».
Évaluation de référence d'un produit	Les résultats de l'évaluation du « produit de référence ».

4. Prérequis

4.1. Analyse d'impact différentielle

Pour définir clairement ce qui distingue chacun des produits de la Gamme, un document appelé *Analyse d'Impact Différentielle* (AID) doit être rédigé par le développeur de la gamme. Ce document doit permettre d'identifier les points communs à l'ensemble des produits de la gamme ainsi que leurs différences.

Ce document se rapproche, par le contenu attendu, du Rapport d'Analyse d'Impact demandé dans la procédure de continuité de l'assurance.

4.2. Choix du produit de référence

Le développeur doit sélectionner le produit de référence parmi la gamme de produits.

Si un seul produit ne peut représenter toute la gamme, il conviendra de choisir les produits de référence permettant de couvrir toute la gamme, ou à défaut de limiter la portée de la gamme.

4.3. Stratégie de réutilisation

Le développeur doit fournir un argumentaire décrivant une *Stratégie de Réutilisation* de tests basée sur l'AID. Cette *Stratégie de Réutilisation* vise à justifier qu'un sous-ensemble des tests peut être effectué sur une partie des produits de la gamme pour valider les comportements de tous ou d'une partie des produits de la gamme.

Dans ce document, le développeur fournit également la justification de son choix du, ou des produits de référence.

4.4. Fournitures

Outre le produit de référence, qui fait partie des fournitures, le développeur doit tenir à disposition de l'évaluateur l'ensemble des produits déclinés. A tout moment lors de l'évaluation, le CESTI pourra demander l'accès à n'importe quel produit décliné. Le CESTI choisit le(s) produit(s) à tester et justifie son choix dans son rapport.

5. Application de la méthodologie d'évaluation

5.1. Aux Critères Communs

Etape 1: Demande d'évaluation d'une gamme de produits

Le développeur soumet la demande de certification, accompagnée des informations référencées dans le chapitre 4.

Le CESTI détermine ensuite la charge de travail pour les classes ATE et AVA, en se basant sur la *Stratégie de Réutilisation* fournie par le développeur. Les éléments présents dans l'AID seront également pris en considération par le CESTI afin de déterminer la charge de travail complémentaire pour les classes ADV, AGD et ALC.

Remarque : À tout moment, le CESTI, ou le centre de certification, peut décider que le produit de référence n'est pas approprié et demander qu'une charge de travail supplémentaire soit allouée pour permettre la réalisation de tests complémentaires sur la gamme.

Le commanditaire peut alors décider de restreindre le périmètre de l'évaluation au(x) seul(s) produit(s) de référence préalablement identifiés.

Etape 2: Evaluation du produit de référence

Le centre d'évaluation mène les travaux d'évaluation sur le(s) produit(s) de référence, conformément aux critères d'évaluation sélectionnés et au niveau d'assurance visé pour la certification.

Etape 3: Evaluation du produit décliné

En complément de l'évaluation du ou des produits de référence l'évaluateur doit réaliser les tâches suivantes :

- ASE
  La cible de sécurité doit clairement identifier la gamme de produits et ses composants.
- ADV
  L'évaluateur doit s'assurer que l'AID est complet et ne présente pas d'erreur.

- AGD
  L'évaluateur doit vérifier que les classes AGD_OPE et AGD_PRE prennent en compte la gamme de produits.
- ALC
  Chaque produit de la gamme de produits doit être identifié de façon unique. Les références de chacun des produits de la gamme doivent être décrites avec précision.

  L'évaluateur doit vérifier que le cycle de vie du produit de référence s'applique ou non aux produits déclinés.

  Toute différence dans le périmètre du cycle de vie devra être évaluée.
- ATE
  FUN, COV, DPT
  L'évaluateur s'assure que le ou les produit(s) de référence, choisi(s) par le développeur, est (sont) un (des) bon(s) candidat(s) pour l'évaluation en s'appuyant sur la justification fournie par le développeur.

  L'évaluateur vérifie la *Stratégie de réutilisation* définie par le développeur et donne son accord. Il doit être montré que tous les sous-systèmes et modules de la TSF, les TSFIs, et les SFR *enforcing* ayant une adhérence aux caractéristiques distinguant les produits de la gamme ont été testés indépendamment.

- ATE_IND
  La vérification de la conformité par le CESTI doit également bénéficier de la *Stratégie de réutilisation* qu'il a validée.

  Des tests, identifiés comme non requis par le développeur dans la *Stratégie de réutilisation,* peuvent toutefois se révéler nécessaires afin de confirmer la complétude et la pertinence de l'*Analyse d'impact différentielle*. Si des différences de comportements sont observées, la pertinence de l'*Analyse d'impact différentielle* peut être remise en cause.
- AVA
  La *Stratégie de réutilisation,* validée par le CESTI, doit permettre à ce dernier d'optimiser la charge concernant les tests de pénétration : seuls les tests ayant une adhérence aux caractéristiques distinguant les produits de la gamme devront être joués par le CESTI sur les produits déclinés.

Etape 4: Certification

Afin d'éviter de multiples certificats, un unique certificat sera émis pour une gamme de produits.

5.2. A la certification de sécurité de premier niveau

Etape 1: Demande d'évaluation d'une gamme de produits

Le développeur prépare les éléments prérequis, référencés dans le chapitre 4. Le CESTI détermine ensuite la charge de travail complémentaire pour couvrir la gamme en se basant sur la *Stratégie de réutilisation*. Les éléments présents dans l'AID seront également pris en considération par le CESTI afin de déterminer la charge de travail complémentaire pour l'analyse de la conformité.

Le développeur peut ensuite soumettre la demande de certification.

Remarque : À tout moment, le CESTI, ou le centre de certification, peut décider que le produit de référence n'est pas approprié et demander qu'une charge de travail supplémentaire soit allouée pour permettre l'évaluation de la gamme de produits.

Le commanditaire peut alors décider de restreindre le périmètre de l'évaluation au(x) seul(s) produit(s) de référence préalablement identifiés.

Etape 2: Evaluation du produit de référence

Le centre d'évaluation mène les travaux d'évaluation sur le produit de référence, conformément à la procédure d'évaluation.

Etape 3: Evaluation du produit décliné

L'évaluateur doit s'assurer que l'AID est complet et ne présente pas d'erreur.

Chaque produit de la gamme de produits doit être identifié de façon unique. Les références de chacun des produits de la gamme doivent être décrites avec précision par le développeur.

La *Stratégie de réutilisation*, validée par le CESTI, doit permettre à ce dernier d'optimiser la charge concernant les tests de pénétration : seuls les tests ayant une adhérence aux caractéristiques distinguant les produits de la gamme devront être joués par le CESTI sur les produits déclinés.

Etape 4: Certification

Afin d'éviter de multiples certificats, un unique certificat sera émis pour une gamme de produits.