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 12 Juillet 2024

N° 1248 **/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CSPN-CER-P-02 v5.0**

PROCEDURE

Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau

Application **:** le 1er Septembre 2024

Diffusion **:** Publique.

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

Annaïg ANDRO

SUIVI DES MODIFICATIONS

Version	Date	Modifications
Phase expérimentale	28 août 2008	Première rédaction pour la phase expérimentale, abrogée par la présente procédure.
1.0	30 mai 2011	Fin de la phase expérimentale. Changement de dénomination de l'organisme de certification (ANSSI), mise au format « Instruction » et améliorations de forme.
1.1	23 avril 2014	Réorganisation des sous-chapitres des chapitres 3.2 et 4. Au chapitre 3.3, ajout du cas où un générateur de nombres aléatoires est utilisé. Précisions, au chapitre 4, des tâches de l'évaluateur concernant la phase 3 (analyse de la documentation), la phase 6 (résistance des mécanismes/fonctions) et la phase 10 (évaluation de la cryptographie). Ajout au chapitre 4 d'une nouvelle phase (phase 7 bis) pour traiter le cas des produits nécessitant des privilèges d'exécution particuliers.
2.0	6 septembre 2018	Mise à jour de la table de cotation au chapitre 4.6, en cohérence avec la version 3.1 révision 3 du document Common Methodology for Information Technology Security Evaluation : Evaluation Methodology. Modification du type de document, correspondant initialement à l'instruction ANSSI-CSPN-CER-I-02.
3.0	18 mars 2019	§5.6 « Résistance des mécanismes/fonctions » - Corrections des tableaux
4.0	28 mars 2020	Clarifications liées à l'analyse de vulnérabilités publiques dans des composants tiers du produit soumis à évaluation. Clarifications liées à l'interprétation des cotations.
5.0	12 juillet 2024	Ajout de la justification de conformité à la norme EN 17640:2022 *Fixed-time cybersecurity evaluation methodology for ICT products*. Remplacement du référentiel cryptographique RGS_B par ANSSI-PG-083. Simplification (réduction du nombre de phases, suppression des doublons internes et avec d'autres documents du centre de certification).

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

Cette procédure 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 procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.cyber.gouv.fr).

TABLE DES MATIERES

1 Objet de la procédure 4
2 Contexte 4
3 Définitions 6
4 Tâches d'évaluation 7
4.1 Fournitures 9
4.1.1 Fournitures documentaires obligatoires au démarrage du projet d'évaluation 9
4.1.2 Fournitures documentaires facultatives 9
4.2 Phase 1 - Analyse de la cible de sécurité et des spécifications cryptographiques 10
4.3 Phase 2 – Installation et mise en œuvre du produit 10
4.4 Phase 3 – Analyse de la documentation et des processus de développement 10
4.5 Phase 4 – Analyse de la conformité des fonctions de sécurité et des mécanismes cryptographiques 11
4.6 Phase 5 – Analyse de la résistance 12
4.6.1 Recherche de vulnérabilités sur le produit (tests de pénétration) 12
4.6.2 Recherche de vulnérabilités induites par le produit sur son système hôte 16
4.7 Résultats de l'évaluation 16
ANNEXE A. Références 17
ANNEXE B. Conformité à EN 17640 18

1 Objet de la procédure

La présente procédure fixe les critères d'évaluation pour une certification de sécurité de premier niveau (CSPN).

2 Contexte

Les présents critères ont été définis par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour permettre l'évaluation, en temps contraint, des fonctions de sécurité proposées par des produits matériels, logiciels ou mixtes visant une CSPN.

Le processus d'évaluation garantit l'atteinte des objectifs ci-dessous :

- vérifier que le produit est conforme à sa spécification en ce qui concerne sa sécurité ;
- déterminer l'efficacité des fonctions de sécurité pour la protection :
    - des biens sensibles définis dans la cible de sécurité ;
    - du système hôte hébergeant le produit.

Hormis les cas où le produit n'utilise pas de mécanismes cryptographiques, deux objectifs supplémentaires sont recherchés :

- vérifier la conformité des mécanismes au référentiel [ANSSI-PG-083] ou [SOG_IS ACM] ;
- vérifier la conformité de l'implémentation de ces mécanismes.

Pour ce faire, le centre d'évaluation s'appuie sur toutes les informations auxquelles il peut avoir accès, notamment, sur la cible de sécurité du produit et sur le produit lui-même. Il consigne les résultats de l'évaluation dans un rapport technique d'évaluation (RTE). Le centre de certification s'appuie sur ce RTE pour proposer ou non la certification de sécurité de premier niveau du produit.

Ces critères peuvent être complétés par des notes d'application spécifiques, applicables à certains produits ou à des cas particuliers.

3 Définitions

Ce chapitre contient les définitions des termes techniques utilisés avec une signification spécifique à ce document. Les termes techniques utilisés dans le présent document qui ne sont pas définis dans ce chapitre sont employés dans un sens conforme à leur acception courante. Le lecteur pourra également se reporter aux définitions de [CER-P-01].

Administrateur (*administrator*) : personne en contact avec le produit et responsable de son maintien en condition d'exploitation.

Configuration (*configuration*) : sélection de l'un des ensembles de combinaisons possibles de caractéristiques d'une cible d'évaluation.

Conformité (*correctness*) : propriété d'une représentation d'une cible d'évaluation qui fait qu'elle reflète exactement la cible de sécurité présentée pour ce produit.

COTS *(Commercial Off-The-Shelf)* **: produit développé et commercialisé en série** (dit aussi « sur étagère »). Un produit soumis à évaluation peut inclure des composants de type COTS, par exemple un processeur ou une librairie propriétaire.

Efficacité (*effectiveness*) **ou résistance** : propriété d'une cible d'évaluation qui représente la mesure dans laquelle elle assure la sécurité dans le contexte de son exploitation réelle ou prévue. L'analyse de la résistance consiste à la fois à recenser les vulnérabilités potentielles présentes sur le produit, mais également à mesurer la capacité du produit à contenir une attaque qui en tirerait parti. Il est nécessaire pour cette analyse de prendre en considération le niveau de ressources nécessaires à un attaquant pour réussir chaque attaque considérée. Outre l'analyse de résistance propre au produit, la CSPN exige également de vérifier, de façon transverse, que le produit évalué ne constitue pas un vecteur d'attaque pour son environnement.

Environnement d'exploitation (*operational environment*) : mesures d'organisation, procédures et normes qui doivent être utilisées au cours de l'exploitation d'une cible d'évaluation.

Environnement TI (*IT environment*) : Environnement lié aux technologies de l'information (p.ex. machines informatiques, système d'exploitation, base de données, réseau, etc.) entourant le produit évalué.

Exigences concernant le contenu et la présentation (*requirements for content and presentation*) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation, qui explicite ce que chaque élément de documentation identifié comme relevant de cette phase ou de cet aspect doit contenir, et comment les informations qu'il contient doivent être présentées.

Exploitation (*operation*) : processus d'utilisation d'une cible d'évaluation.

Facilité d'emploi (*ease of use*) : aspect de l'estimation de l'efficacité d'une cible d'évaluation consistant à assurer qu'elle ne peut pas être configurée ou utilisée d'une manière non sûre, mais qu'un administrateur ou un utilisateur final pourrait raisonnablement croire sûre.

Menace (*threat*) : action ou événement susceptible de porter préjudice à la sécurité.

Réalisation (*implementation*) : phase du processus de développement dans laquelle la spécification détaillée d'une cible d'évaluation est traduite en matériels et logiciels réels.

Tâches de l'évaluateur (*evaluator actions*) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation identifiant ce que l'évaluateur doit effectuer pour vérifier les informations fournies par le commanditaire de l'évaluation, et les actions complémentaires qu'il doit effectuer.

Tests de pénétration (*penetration testing*) : tests effectués par un évaluateur sur une cible d'évaluation pour confirmer si oui ou non les vulnérabilités identifiées sont réellement exploitables en pratique.

Utilisateur final (*end-user*) : personne en contact avec une cible d'évaluation qui n'utilise que ses capacités opérationnelles.

Vulnérabilité (*vulnerability*) : faiblesse de la sécurité d'une cible d'évaluation (due par exemple à des défauts dans l'analyse, la conception, la réalisation ou l'exploitation).

4 Tâches d'évaluation

Le présent chapitre fixe les tâches d'évaluation qui visent à vérifier la conformité du produit à ses spécifications. La base d'évaluation est constituée par une cible de sécurité, qui doit contenir les éléments nécessaires tels que spécifiés dans ce document. Le contenu et la présentation des preuves de ces activités doit suivre [NOTE-01].

Les tâches sont organisées en « phases » mais cela ne signifie pas qu'elles doivent être effectuées de façon séquentielle. Comme précisé dans la figure ci-dessous, l'analyse de la documentation se fait en parallèle d'autres activités – en revanche, les constats de toutes les phases alimentent la phase 5.

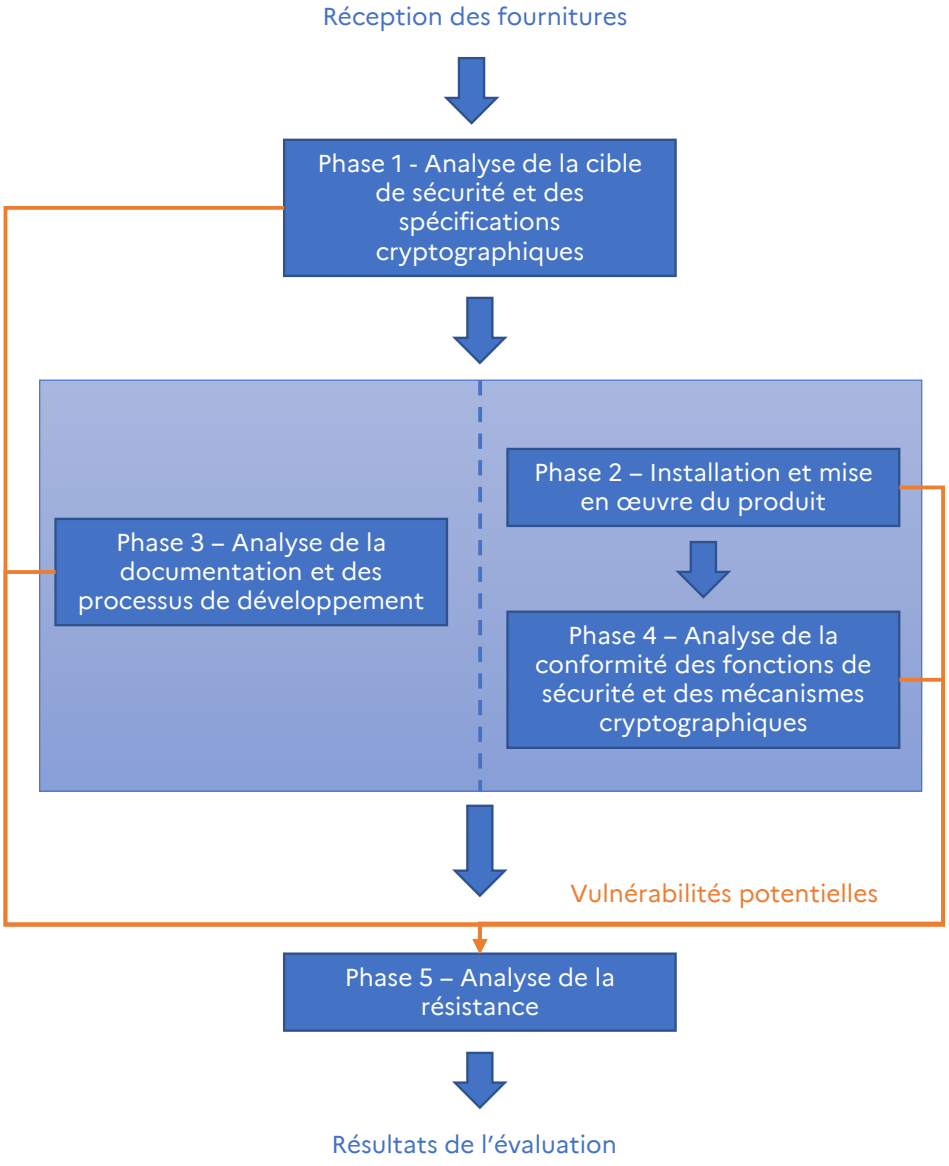

Figure 1 : Séquencement des phases d'évaluation

4.1 Fournitures

4.1.1 *Fournitures documentaires obligatoires au démarrage du projet d'évaluation*

4.1.1.1 Cible de sécurité et fournitures cryptographiques

Comme le prévoit [CER-P-01], le commanditaire doit fournir à l'évaluateur, au démarrage du projet d'évaluation, la cible de sécurité et les éventuelles fournitures spécifiques pour l'analyse cryptographique[1].

4.1.1.2 Documentation opérationnelle

La **documentation utilisateur ou d'exploitation** doit permettre aux utilisateurs de mettre en œuvre, de façon sûre, les fonctions de sécurité décrites dans la cible de sécurité du produit. Elle doit également permettre à l'utilisateur de se positionner dans le contexte d'utilisation décrit dans la cible.

La **documentation d'administration** doit décrire les fonctions relevant des activités administration dédiées à la sécurité. Elle doit décrire tous les paramètres de sécurité, tous les événements relatifs à la sécurité relevant des fonctions d'administration. Elle doit décrire, d'une façon suffisamment détaillée pour leur utilisation, les procédures relevant de l'administration de la sécurité. Elle doit donner des recommandations ou avertissements permettant l'utilisation cohérente et efficace des fonctions de sécurité du produit et sur la façon dont ces fonctions interagissent. La documentation d'administration doit décrire comment le produit est administré de façon sûre.

La **documentation d'installation et de configuration** doit décrire la façon dont le système ou le produit devra être installé et, le cas échéant, la façon dont il devra être configuré. Si différentes configurations sont possibles, elle doit permettre d'installer le produit dans les différentes configurations couvertes par l'évaluation. L'impact des configurations sur la sécurité doit être décrit. Si une fonction dédiée à la sécurité peut être désactivée ou modifiée pendant le démarrage, l'exploitation normale ou la maintenance, cela doit être décrit.

Tous les documents liés au produit doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis. La documentation doit donner les recommandations ou avertissements nécessaires vis-à-vis des différentes catégories d'utilisateurs concernés. L'identification de la documentation doit être non ambiguë.

4.1.2 *Fournitures documentaires facultatives*

4.1.2.1 Procédures liées au cycle de vie

Les **procédures de livraison** doivent garantir l'authenticité et l'intégrité du produit livré.

Les **procédures de génération du système** peuvent être consultées au titre de l'entretien avec les développeurs (Phase 3). Ces procédures doivent garantir l'authenticité et l'intégrité du produit généré.

Peuvent s'ajouter à ces procédures d'autres documents, par exemple des procédures de **gestion de configuration** ou de **sécurité de l'environnement de développement**.

[1] Sauf si le produit ne contient aucun mécanisme cryptographique.

4.2 Phase 1 - Analyse de la cible de sécurité et des spécifications cryptographiques

Revue documentaire

E_CSPN_P1_1. Vérifier que la cible de sécurité respecte [NOTE-09].

E_CSPN_P1_2. Vérifier que les spécifications cryptographiques respectent [CRYPTO].

E_CSPN_P1_3. Vérifier qu'il n'y a pas d'incohérence entre la cible de sécurité et les spécifications cryptographiques.

Remarque : ces exigences reprennent les work units 1, 2 et 3 du §6.1, ainsi que la work unit 1 du §6.3 et la work unit 1a du §6.4 de [FitCEM], en les raffinant au regard des exigences du centre de certification national. La work-unit 1b du §6.4 de [FitCEM] n'est pas applicable au centre de certification national, qui ne met pas en œuvre le concept de Fit PP.

4.3 Phase 2 – Installation et mise en œuvre du produit

Installation de la plate-forme d'évaluation (ou plateforme de tests)

E_CSPN_P2_1. Installer la plate-forme d'évaluation et/ou s'assurer qu'elle est bien installée. Cette plate-forme doit être représentative de l'environnement dans lequel le produit est normalement utilisé, dans la limite des possibilités allouées au projet d'évaluation. La mise en place de la plate-forme ne fait pas partie de l'évaluation.

E_CSPN_P2_2. Lorsque l'environnement technique est décrit de façon générique, l'évaluateur ne peut envisager de tester le produit sur toutes les plates-formes possibles. Soit il en détermine une particulière en accord avec le commanditaire ; soit il procède conformément à la note [ANSSI-CC-NOTE-21] avec d'éventuels compléments de charges associés. Dans tous les cas, la cible de sécurité sera modifiée pour décrire le ou les environnements choisis.

Installation du produit

E_CSPN_P2_3. Vérifier que la documentation d'installation et de configuration existe, et vérifier qu'elle satisfait les exigences du paragraphe 4.1. Si la documentation existe en plusieurs langues, utiliser la documentation écrite dans la même langue que la cible de sécurité. Seul le français et l'anglais sont acceptables, si ce n'est pas le cas, une traduction des documents est nécessaire.

E_CSPN_P2_4. Procéder à l'installation du produit dans sa configuration typique (installation recommandée par la documentation d'installation ou par le processus d'installation).

Mise en état sécurisé

E_CSPN_P2_5. Vérifier que l'installation aboutit à un état sécurisé du produit. Si ce n'est pas le cas, l'évaluateur est autorisé à demander des mises à jour de la documentation, dans les limites de la [NOTE-20].

Remarque : ces exigences reprennent les work units 1, 2 et 3 du §6.6 de [FitCEM], en les raffinant au regard des exigences du centre de certification national.

4.4 Phase 3 – Analyse de la documentation et des processus de développement

E_CSPN_P3_1. **Analyse de la documentation**Si tout ou partie de la documentation est indisponible, indiquer si le produit peut néanmoins être configuré, administré et utilisé

conformément à ce qui est décrit dans la cible de sécurité, en prenant en compte la compétence que cela demanderait de la part des utilisateurs concernés[2].

Remarque : ces exigences reprennent le work unit 1 du §6.5 de [FitCEM], en la raffinant au regard des exigences du centre de certification national.

Entretien avec les développeurs

E_CSPN_P3_2. Acquérir auprès des développeurs de l'information sur l'ensemble des critères analysés. Cette tâche est facultative. Elle implique que les développeurs soient disponibles et acceptent cette démarche. L'évaluateur aura intérêt à la réaliser en début de projet et à la compléter ponctuellement en cours de projet si de nouvelles questions apparaissent.

4.5 Phase 4 – Analyse de la conformité des fonctions de sécurité et des mécanismes cryptographiques

Plan de test

E_CSPN_P4_1. Définir un plan de test afin d'établir la conformité de chaque fonction de sécurité listée dans la cible de sécurité, et de chaque mécanisme cryptographique listé dans les spécifications cryptographiques. Le plan de test devra :

a. lister les éventuels critères d'acceptation visés pour les fonctions ou mécanismes testés ;

b. décrire quelles activités seront menées pour la vérification de conformité de chaque fonction ou mécanisme[3] ;

c. décrire quelles méthodes internes/externes et quels outils seront utilisées, en justifiant leur pertinence (notamment, pour les outils, en justifiant la suffisance et la complétude de leurs résultats par rapport aux attendus, et en complétant leur utilisation par des tests manuels si nécessaire).

Le plan de test devra prendre en compte les éventuelles exigences du centre de certification national propres au type de produit ou à la technologie concernée. L'analyse des mécanismes cryptographiques, par exemple, doit respecter les exigences que [CRY-P-01] impose pour la vérification de conformité à [ANSSI-PG-083] ou [SOG_IS ACM][4].

[2] L'évaluateur s'aidera des définitions suivantes :

- utilisateur grand public : pas de compétence particulière en informatique ;
- utilisateur confirmé : connaissance des principaux concepts de l'informatique ;
- administrateur : connaissance fine des principaux concepts de l'informatique et des réseaux, capacité à configurer et administrer un parc d'ordinateurs reliés en réseau ;
- expert : expert dans le domaine du produit (typiquement, l'évaluateur).

[3] On parle de plan de tests car la vérification s'appuie essentiellement sur des tests. Dans certains cas, il est possible de s'appuyer sur des activités additionnelles, comme par exemple des revues de configuration ou de code source (lorsque disponible). Des activités alternatives peuvent également être proposées lorsqu'il n'est pas possible d'effectuer un test du mécanisme visé.

[4] La vérification de la conformité des mécanismes cryptographiques et des générateurs de nombres aléatoires par rapport aux exigences du référentiel technique de l'ANSSI [ANSSI-PG-083] ou [SOG_IS ACM] se fait par une analyse documentaire, tandis que la vérification de la conformité de la mise en œuvre de ces mécanismes par le produit peut se faire de plusieurs façons :

- par comparaison des résultats de traitements cryptographiques réalisés par le produit par vis-à-vis d'une implémentation de référence. Cela implique que soient mis à disposition de l'évaluateur soit plusieurs entrées/sorties de référence (clé, clair, chiffré), soit les moyens de récupérer un ensemble d'entrées/sorties et de secrets qui pourront ensuite être injectés dans un simulateur logiciel pour réaliser les mêmes traitements que le produit, afin de pouvoir faire les comparaisons ;

E_CSPN_P4_2. Si nécessaire, obtenir la validation du plan de tests par le centre de certification[5].

Campagne de tests

E_CSPN_P4_3. Mettre en œuvre les tests planifiés et s'assurer que les résultats permettent effectivement de se prononcer quant à la conformité des fonctions et mécanismes cryptographiques.

Remarque : ces exigences reprennent les work units 1, 2 et 3 du §6.7 ainsi que les work units 1 et 2 du §6.12 de [FitCEM], en les raffinant au regard des exigences du centre de certification national.

4.6 Phase 5 – Analyse de la résistance

4.6.1 *Recherche de vulnérabilités sur le produit (tests de pénétration)*

Identification de la surface d'attaque

E_CSPN_P5_1. Analyser la surface d'attaque, en prenant en compte les possibles configurations non sûres du produit induites par des problèmes de facilité d'emploi[6].

E_CSPN_P5_2. Le centre d'évaluation doit s'assurer que les mesures techniques sont suffisamment précises et réalistes pour qu'un utilisateur final du certificat soit en mesure d'être effectivement protégé contre les menaces identifiées dans la cible de sécurité. Ainsi, le centre d'évaluation ne doit pas écarter les chemins d'attaque :

a. passant par l'environnement TI. En particulier, des tests de pénétration peuvent démontrer que certaines mesures sur l'environnement TI ne sont pas pertinentes ou ne sont pas suffisantes ;
b. trouvant leur origine dans des problèmes de facilité d'emploi du produit, en particulier si le produit :
    i. peut donner une fausse impression de sécurité à un administrateur ou un utilisateur final ;
    ii. inclut des fonctions intrinsèquement non-sûres, menant potentiellement à une vulnérabilité exploitable ;
    iii. est complexe à mettre dans un état sûr, au point qu'il est raisonnable de penser qu'il peut être mal configuré en pratique.

Inventaire des vulnérabilités connues

E_CSPN_P5_3. Recenser les vulnérabilités connues spécifiques au produit[7].

- par analyse du code source avec éventuellement des tests unitaires de certaines fonctions (par exemple, vérifier qu'une fonction AES réalise bien un AES) ;
- en vérifiant que le produit à tester communique de façon chiffrée avec un équipement de référence, dans le cas où le produit à tester est un système communicant.

Plusieurs approches étant possibles, l'évaluateur décrira celles qu'il a adoptées pour se convaincre de la conformité de l'implémentation par rapport aux spécifications.

[5] La validation du centre de certification peut par exemple être requise lorsque la cible de sécurité inclut de nouvelles technologies ou de nouvelles fonctionnalités de sécurité, cf. Annexe B de [CER-P-01]

[6] Le produit peut par exemple présenter des interfaces ou des fonctions non décrites dans la cible de sécurité.

[7] Cela suppose qu'un suivi des vulnérabilités est effectué

- par le développeur (pour les composants qu'il développe), et
- par les développeurs des composants tiers (COTS ou open source).

Pour chaque vulnérabilité :

a. décrire les conditions, techniques et effets de la réalisation de la vulnérabilité ;

b. chercher si un correctif, officiel ou non, ou une méthode de contournement, permettent de limiter les effets de la vulnérabilité.

E_CSPN_P5_4. Recenser les vulnérabilités connues génériques : il s'agit typiquement de vulnérabilités découvertes sur des produits similaires ou sur le type de technologie utilisée et pour lesquelles il n'existe pas d'information prouvant que le produit concerné s'en prémunit.

Tests de pénétration

E_CSPN_P5_5. Définir une stratégie de tests permettant de se prononcer sur l'intégralité de la surface d'attaque dans le temps de l'évaluation et justifiant les priorités choisies par l'évaluateur[8] . La stratégie de tests s'appuie sur :

a. les constats des phases 1 à 4 ;

b. la surface d'attaque ;

c. les vulnérabilités connues (spécifiques au produit ou génériques au type de produit ou à la technologie utilisée) ;

d. la recherche de vulnérabilités additionnelles, dans toute partie du produit et par tout moyen accessible à l'évaluateur (documentation, accès à un produit « de production » et/ou « ouvert », accès éventuel au code source).

E_CSPN_P5_6. Effectuer les tests en modifiant la stratégie si nécessaire en fonction des informations découvertes[9].

E_CSPN_P5_7. Définir les scénarios d'attaque pouvant tirer parti des vulnérabilités découvertes (ne sont considérées comme attaques complètes que celles qui permettent de compromettre un des biens sensibles définis dans la cible de sécurité). Il s'agit :

a. de proposer une cotation de l'exploitation de chaque vulnérabilité, en utilisant les tables de cotation qui suivent ;

b. de donner une cotation de la résistance globale du produit du point de vue de la sécurité, en s'appuyant sur les cotations des vulnérabilités découvertes ;

L'évaluateur est autorisé à rendre un verdict d'échec s'il n'est pas certain de disposer de la liste exhaustive des vulnérabilités connues sur le produit ou ses composants tiers.

L'évaluateur est également autorisé à rendre un verdict d'échec si la liste de vulnérabilités connues est trop importante pour être analysée dans le temps de l'évaluation. Afin de mitiger ce risque, l'évaluateur est autorisé à demander au développeur un argumentaire démontrant que les vulnérabilités identifiées sont non-applicables, sans impact, corrigées ou contournables. Attention, l'évaluateur devra cependant se prononcer sur la pertinence de cet argumentaire, qui ne remplace pas sa propre analyse.

[8] Ainsi un scénario de menace pourra être écarté car il n'est pas réalisable au regard des hypothèses, mais plus généralement l'évaluateur devra prioriser ses scénarios de façon à s'assurer que les scénarios les plus « faciles » ont bien été vérifiés avant de tenter des scénarios plus complexes. Les vulnérabilités connues peuvent par exemple être priorisées selon des critères de choix comme la faisabilité, l'exploitabilité, l'absence de correctif, la gravité (gain attendu pour l'attaquant) …

[9] Le principe du test de pénétration est que la découverte d'informations au cours des tests est susceptible de faire changer les priorités de l'évaluateur. Par exemple :

- la découverte de mécanismes de cloisonnement forts permettra de baisser la priorité de plusieurs scénarios qui semblaient pertinents à première vue, dans la mesure où ils deviennent désormais plus difficiles à exploiter ;
- à l'inverse, la découverte d'une exécution de code dans un processus non privilégié peut pousser l'évaluateur à creuser ce point et chercher une élévation de privilège additionnelle, quitte à baisser la priorité d'un autre test.

c. en fonction des cotations obtenues, de donner un avis d'expert sur la résistance des fonctions et la résistance globale du produit à des attaques.

Remarques : Les tableaux suivants constituent le modèle par défaut permettant le calcul de cotations en CSPN. L'évaluateur consultera la [CEM] pour plus d'information sur leur utilisation. Des tables de cotation spécifiques peuvent cependant être redéfinies pour certaines catégories de produits. En particulier :

- *les cartes à puce et produits similaires devront être évaluées selon les tables de cotation du document [JIL_HW].*
- *les produits de type « équipement matériel avec boîtier sécurisé » devront être évalués selon les tables de cotation du document [JIL_HWD].*

En plus de ces tables de cotations, l'évaluateur devra prendre en compte le document [CRY-P-01] pour l'analyse des mécanismes mettant en œuvre des algorithmes cryptographiques ou des générateurs de nombres aléatoires.

En cas de doute concernant le choix de la table de cotation, l'évaluateur est invité à contacter le centre de certification national.

Facteur	*Valeurs*	
Temps mis pour l'identification et l'exploitation	<= 1 jour	0
	<= 1 semaine	1
	<= 2 semaines	2
	<= 1 mois	4
	<= 2 mois	7
	<= 3 mois	10
	<= 4 mois	13
	<= 5 mois	15
	<= 6 mois	17
	> 6 mois	19
Expertise de l'attaquant	Profane	0
	Compétent	3
	Expert	6
	Multiples experts	8
Connaissance nécessaire à l'attaquant	Aucune[10]	0
	Information restreinte	3
	Information sensible	7
	Information critique	11
Accès au produit par l'attaquant	Pas nécessaire / illimité	0
	Facile	1
	Modéré	4
	Difficile	10
	Aucun	*[11]
Type d'équipement nécessaire[12]	Aucun / standard	0
	Logiciel spécialisé	2

[10] Incluant le recours à de la documentation publique.

[11] Indique que l'attaque n'est pas réalisable du fait des contre-mesures mises en œuvre dans l'environnement opérationnel de la TOE.

[12] Ces valeurs prennent en compte la note d'application 18, ANSSI-CC-NOTE-18, qui diffère de la [CEM]. Dans le cas où une attaque nécessite une intervention physique et l'utilisation de matériel, l'ensemble de l'attaque sera à coter selon la table de cotation de [JIL_HW] ou [JIL_HWD] (le CESTI choisira celui des deux qui semble le plus approprié par rapport au produit évalué).

Si l'attaque est cotée à la valeur	Alors l'attaque est considérée comme exploitable par un attaquant de niveau	La résistance de la TOE est-elle mise en échec ?
0 à 9	Basique	Oui
10 à 13	Basique augmenté	Oui
>= 14 à 19	Moyen	Non

4.6.2 *Recherche de vulnérabilités induites par le produit sur son système hôte*

E_CSPN_P5_8. Evaluer l'impact de l'installation du produit sur la sécurité du système hôte, surtout dans le cas où le produit nécessite des privilèges particuliers[13] :

a. identifier les privilèges ou les conditions de cloisonnement nécessaires sur le système hôte pour que le produit s'exécute correctement ;

b. donner un avis d'expert motivé sur l'impact qu'a le produit sur la sécurité de son système hôte.

Remarque : ces exigences reprennent les work units 1 et 2du §6.10 de [FitCEM], en les raffinant au regard des exigences du centre de certification national.

4.7 Résultats de l'évaluation

L'évaluation d'un produit suivant les critères exposés dans le présent document permet de constater que le produit fournit bien les fonctions de sécurité indiquées dans la cible de sécurité, qu'aucune vulnérabilité de niveau « Basique augmenté » (au sens du chapitre 4.6) n'a pu être exploitée lors de l'évaluation. Cette dernière conclusion doit être prise avec toute la prudence que l'on doit avoir dans le domaine de la sécurité des technologies de l'information. Il n'est en effet pas possible de garantir l'absence de vulnérabilité exploitable dans le produit.

Le plan du RTE est imposé. Il est téléchargeable sur le site de l'ANSSI (www.cyber.gouv.fr), voir [CSPN-NOTE-01].

[13] La notion de « système hôte » est à interpréter par l'évaluateur en fonction du type de produit visé. Par exemple :

- le « système hôte » d'un antivirus pourra être l'OS sur lequel il s'exécute ;
- le « système hôte » d'un pare-feu pourra être le réseau au sein duquel il est déployé.

La notion de vulnérabilité induite est également à interpréter dans le contexte du type de produit visé. Par exemple :

- un antivirus nécessitant des privilèges élevés pourra constituer un vecteur d'élévation de privilège sur l'OS hôte en cas d'exécution de code ;
- un pare-feu permettant le *SSH port forwarding* pourra constituer un vecteur de pivot vers le réseau hôte.

ANNEXE A. Références

Référence	Document
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, version en vigueur.
[ANSSI-PG-083]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.
[CER-P-01]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version en vigueur.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations de générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P-01, version en vigueur.
[NOTE-09]	Contenu et structure de la cible de sécurité CSPN, référence ANSSI-CSPN-NOTE-09, version en vigueur.
[CRYPTO]	Fournitures nécessaires à l'analyse de mécanismes cryptographiques, version en vigueur.
[NOTE-01]	Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau - Contenu et structure du RTE, référence ANSSI-CSPN-NOTE-01, version en vigueur.
[NOTE-20]	Règles relatives à la mise en œuvre des évaluations sécuritaires, référence ANSSI-CC-NOTE-20, version en vigueur.
[AGR-P-01]	Agrément des centres d'évaluation en vue de la Certification de sécurité de premier niveau, référence ANSSI-CSPN-AGR-P-01, version en vigueur.
[CER-F-01]	Dossier d'évaluation en vue d'une Certification de sécurité de premier niveau (CSPN), référence ANSSI-CSPN-CER-F-01, version en vigueur.
[JIL_HW]	*Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices - Version 3.2.1 – February 2024*
[JIL_HWD]	*Joint Interpretation Library - Application of Attack Potential to Hardware Devices with Security Boxes - Version 3.1 November 2023.*
[FitCEM]	*EN 17640 Fixed-time cybersecurity evaluation methodology for ICT product, version 2022.*

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

ANNEXE B. Conformité à EN 17640

La méthode d'évaluation CSPN décrite dans cette procédure est conforme aux exigences de la norme [FitCEM] pour une évaluation de niveau *High*.

Le tableau ci-dessous donne les détails de la traçabilité entre l'EN 17640 et la CSPN.

Tâche d'évaluation [FitCEM]	Correspondance CSPN
6.1 - Completeness check	**6.1.1, 6.1.2, 6.1.4 : [CER-P-01]** décrit les éléments requis pour toute demande d'évaluation CSPN (§5), ainsi que les responsabilités du commanditaire de fournir ces éléments (§9.1). Voir également *§3* du présent document. **[NOTE-20]** précise les exigences de mise à disposition du produit à évaluer (calendrier, complétude...). Aux *§3.5.2 à 3.5.5*. **6.1.3 : [AGR-P-01]** prévoit que le CESTI dispose des "connaissances techniques et expérience nécessaires pour exercer les activités correspondantes" au sein de son domaine d'agrément. Le CESTI s'engage en signant **[CER-F-01]** lors de l'enregistrement, à s'assurer que "les travaux objet de l'évaluation correspondent totalement à sa portée d'agrément ».
6.2 - FIT Protection Profile Evaluation	La CSPN n'implémente pas cette activité optionnelle (cf. **[FitCEM]**, Table 1) car elle n'utilise pas le concept de profil de protection pour l 'instant (elle autorise les commanditaires à s'inspirer de documents intitulés cibles génériques ou profils de protection, mais la conformité à ces documents n'est pas évaluée dans le cadre de l'évaluation).
6.4 - FIT Security Target Evaluation	**6.4.1, 6.4.2, 6.4.4 :** voir Phase 1 du présent document. **6.4.3 :** cf. argumentaire donné en 6.1.
6.5 - Development documentation	**6.5.1, 6.5.2, 6.5.4 :** voir Phases 1 et 3 du présent document[14]. **6.5.3 : [AGR-P-01]** inclut la cryptographie comme domaine d'agrément ; les évaluateurs sont donc audités sur ce type de compétences, ce qui garantit leur capacité à analyser les spécifications cryptographique
6.6 - Evaluation of TOE Installation	**6.6.1, 6.6.2, 6.6.4 :** voir Phase 2 du présent document. **6.6.3** : la capacité à évaluer la cryptographie et à mener des attaques de ce domaine sur le produit est évaluée au titre de la grille de compétences associée à **[AGR-P-01]**. Elle implique la capacité à installer, débugger, ou effectuer des tests fonctionnels sur le produit. Pour cette raison, la procédure d'agrément **[AGR-P-01]** et la grille de compétence associée couvre déjà les compétences liées à cette activité.
6.7 - Conformance testing	**6.7.1, 6.7.2, 6.7.3 :** voir Phase 4 du présent document. **6.7.3 :** cf. argumentaire donné en 6.6.
6.10 - Penetration testing	**6.10.1, 6.10.2, 6.10.4 :** voir Phase 5 du présent document. **6.10.3 :** cf. argumentaire donné en 6.6.
6.12 - Extended crypto analysis	**6.12.1, 6.12.2, 6.12.3** voir Phase 4 du présent document. **6.12.3 :** cf. argumentaire donné en 6.6.

[14] [FitCEM] §6.5.1 précise que cette tâche d'évaluation de la documentation du développement peut s'avérer très chronophage et par conséquent doit être conservée à son minimum, en lui substituant par exemple les tests de pénétration. La CSPN ne conserve, dans la documentation de conception, que les spécifications cryptographiques. Cette mention vise justement les méthodes de type CSPN, qui font le choix de limiter l'analyse de la documentation au minimum et de concentrer l'effort sur les tests de pénétration.