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 28 mars 2020

N° 1436/ANSSI/SDE/PSS/CCN

Référence :

ANSSI-CSPN-CER-P-02_v4.0

PROCEDURE

CRITERES POUR L'EVALUATION EN VUE D'UNE CERTIFICATION DE SECURITE DE PREMIER NIVEAU

Application : Dès son approbation.

Diffusion : Publique.

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

Suivi des modifications

Editions	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.

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

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

TABLE DES MATIERES

1 Objet de la procédure

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

2 Références

[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, version en vigueur.
[RGS_B]	Référentiel général de sécurité, annexes B : [RGS_B1] : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. [RGS_B2] : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques. [RGS_B3] : Règles et recommandations concernant les mécanismes d'authentification.
[CSPN]	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 nombres aléatoires, référence ANSSI-CC-CRY-P-01, version en vigueur
[CRYPTO]	Fournitures nécessaires à l'analyse de mécanismes cryptographiques, version en vigueur.
[CSPN 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.
[JIL_HW]	Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices - Version 3.0 - April 2019
[JIL_HWD]	Joint Interpretation Library - Application of Attack Potential to Hardware Devices with Security Boxes - Version 2.0 (for trial use) - December 2015

3 Champ d'application

3.1 Objectif des présents critères

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 fonctionnalités de sécurité proposées par des produits matériels, logiciels ou mixtes visant une CSPN.

Deux objectifs principaux sont recherchés lors de l'évaluation :

- vérifier que le produit est conforme à sa spécification pour ce qui concerne sa sécurité ;
- déterminer l'efficacité des fonctionnalités de sécurité.

Dans le cas où le produit nécessite des privilèges particuliers pour s'exécuter sur le système hôte, l'évaluation devra également porter sur l'impact de l'installation du produit sur la sécurité du système hôte.

Lorsque des fonctions de sécurité essentielles du produit sont implémentées par des mécanismes cryptographiques, deux objectifs supplémentaires sont recherchés lors de l'évaluation :

- vérifier la conformité des mécanismes cryptographiques aux exigences décrites dans le référentiel technique de l'ANSSI [RGS_B] ;
- vérifier la conformité de la mise en œuvre de ces mécanismes par le produit en se référant à leur description.

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

3.2 But de l'évaluation

L'objectif du processus d'évaluation est de permettre à un centre d'évaluation de vérifier si le produit est conforme à sa spécification, de déterminer l'efficacité des fonctionnalités de sécurité et d'en consigner les résultats dans un rapport technique d'évaluation (RTE).

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.

Le centre de certification s'appuie sur le RTE pour proposer ou non la certification de sécurité de premier niveau du produit.

3.3 Les acteurs de l'évaluation

Le rôle des différents acteurs est précisé dans la procédure ANSSI-CSPN-CER-P-01 (voir [ANSSI-CSPN-CER-P-01]).

4 Fournitures documentaires minimales

4.1 Introduction

Un produit qui fournit de la sécurité (une combinaison de confidentialité, d'intégrité, d'authentification et de disponibilité) doit présenter des caractéristiques de sécurité appropriées. Il est nécessaire de déterminer le degré de confiance qui peut être accordé à ces caractéristiques.

Pour cela, les caractéristiques elles-mêmes doivent être spécifiées au sein d'un document, qui constitue la cible de sécurité de ce produit.

4.2 La cible de sécurité

La cible de sécurité sert à la fois de spécification des fonctions dédiées à la sécurité et de description des liens entre le produit et l'environnement dans lequel celui-ci sera exploité. Sont donc intéressés par la cible de sécurité, non seulement le développeur du produit et les responsables de son évaluation, mais également les personnes chargées de sa gestion, de son achat, de son installation, de sa configuration, de son exploitation et de son emploi.

Le contenu exigé d'une cible de sécurité est le suivant :

a) une identification non ambiguë du produit à évaluer ;
b) une identification du ou des concepteurs du produit ;
c) un argumentaire du produit décrivant l'usage du produit, ainsi que le contexte d'emploi dans lequel il est censé être utilisé ;
d) l'environnement technique dans lequel le produit fonctionne (modèle d'ordinateur, système d'exploitation, etc.) ;
e) les biens sensibles que le produit doit protéger ;

f) les mesures d'environnement ;
g) les menaces contre lesquelles le produit offre une protection ;
h) les fonctionnalités de sécurité implémentées par le produit pour parer les menaces identifiées. Ce sont ces fonctionnalités qui feront l'objet de l'évaluation.

Chacun de ces éléments est décrit plus en détail ci-dessous.

a) Identification non ambiguë du produit

Il doit être possible d'identifier sans ambiguïté le produit qui est évalué, et en particulier sa version.

b) Concepteurs du produit

Il doit être possible d'identifier sans ambiguïté qui est le concepteur du produit. Si certains composants sont fournies par des tiers, ou sont en source ouverte, alors il doit être possible d'identifier sans ambiguïté qui a conçu chaque composant.

c) Argumentaire d'un produit

L'argumentaire d'un produit doit identifier la manière dont il est prévu d'utiliser ce produit, l'environnement prévu pour son utilisation et les menaces supposées dans cet environnement. Il doit également inclure un résumé des caractéristiques de sécurité du produit. Ceci doit inclure les dépendances du produit par rapport à des matériels, des logiciels et/ou des microprogrammes qui ne sont pas fournis avec le produit.

La cible doit également décrire l'environnement dans lequel le produit sera utilisé. Cet environnement n'est pas toujours précisément connu de son développeur : en effet, le produit peut être incorporé dans différents systèmes ou différents environnements. Dans ce cas, il doit être fourni un argumentaire qui donne les informations nécessaires à l'utilisateur final pour décider si ce produit va l'aider à satisfaire aux objectifs de sécurité de son système, et pour définir ce qui reste à faire pour les satisfaire complètement.

c) Environnement technique de fonctionnement du produit

La cible de sécurité doit préciser l'environnement technique attendu pour permettre l'exécution du produit. Il peut s'agir d'un environnement technique générique (par exemple, ordinateur compatible PC sous un système d'exploitation donné) ou d'un environnement dédié (tel modèle d'ordinateur avec telle configuration particulière, etc.).

Lorsque l'environnement technique est décrit de façon générique, l'évaluateur ne peut envisager de tester le produit sur toutes les plates-formes possibles. Il en détermine une particulière, éventuellement en accord avec le commanditaire, pour procéder à l'évaluation. La spécification de cette plate-forme doit clairement apparaître dans le RTE et être indiquée dans le rapport de certification.

d) Biens sensibles devant être protégés

La cible de sécurité doit décrire les biens sensibles que les fonctions de sécurité implémentées dans le produit sont destinées à protéger. Elle doit préciser la protection attendue pour ces biens (confidentialité, intégrité, disponibilité, authentification). Pour protéger des biens sensibles, le produit doit parfois lui-même gérer des informations qui deviennent également des biens sensibles. Par exemple, les données utilisateurs peuvent être protégées en confidentialité par une fonction de chiffrement, qui utilisera normalement une clé de chiffrement. Cette clé de chiffrement est également un bien sensible du produit.

e) Mesures d'environnement

Pour répondre à ses spécifications de sécurité, il est possible que le produit doive être utilisé dans un environnement particulier et avec une organisation particulière.

Ces mesures d'environnement devront être décrites dans la cible de sécurité. Ceci doit inclure les mesures de sécurité logiques, physiques, organisationnelles, relatives au personnel et les technologies de l'information (TI) requises pour exploiter le produit.

Elles devront être « réalistes » par rapport à l'emploi prévu du produit. Ainsi, un produit bureautique grand public ne pourra pas revendiquer une mesure d'environnement imposant son utilisation dans une zone à accès contrôlé sous surveillance 24/24, etc.

f) Description des menaces

La cible de sécurité doit décrire les menaces couvertes par les fonctions de sécurité. Une menace peut se caractériser par les éléments suivants :

- un acteur (utilisateur autorisé, administrateur, etc.) ;
- un type de menace (erreur de saisie, malveillance, etc.) ;
- un bien impacté.

Par exemple, le fait qu'un utilisateur puisse réaliser une mauvaise saisie modifiant le comportement de la fonction de sécurité X constitue une menace.

g) Spécification des fonctions dédiées à la sécurité

La cible de sécurité doit inclure une spécification des fonctions dédiées à la sécurité que le produit doit fournir. Ces fonctions peuvent être déclarées explicitement, ou faire référence à une norme acceptée qui définit une fonctionnalité de sécurité.

Pour les fonctions qui reposent sur une base de connaissance[1] ou sur un moteur d'analyse de code, l'évaluation ne porte pas sur la qualité[2] de cette base de connaissance ou des techniques d'analyse mises en œuvre par le moteur. En effet, ce type d'analyse n'entre pas dans le cadre d'une évaluation CSPN au vue de la charge impartie à ce processus d'évaluation.

Une cible de sécurité peut s'appuyer sur un ou plusieurs documents normatifs relatifs à la sécurité, soit en y faisant référence, soit en les incluant. Lorsque les normes permettent des options, les options choisies doivent être clairement identifiées. Lorsqu'une norme ne fournit pas toutes les informations requises, les informations complémentaires nécessaires doivent être explicitement fournies dans la cible de sécurité.

Dans le cas d'un produit, les fonctions dédiées à la sécurité doivent être reliées aux modes prévus d'utilisation du produit.

La spécification des fonctions dédiées à la sécurité doit également montrer en quoi les fonctions sont adaptées pour contrer les menaces identifiées. Cette mise en correspondance doit inclure toutes les dépendances envers d'autres fonctions dédiées à la sécurité et d'autres mesures ne relevant pas de la sécurité des technologies de l'information (TI), supposément fournies par l'environnement.

Du point de vue de l'évaluation, la spécification des fonctions dédiées à la sécurité est la partie la plus importante de la cible de sécurité. Ces fonctions doivent au moins être spécifiées dans un mode informel en langage naturel.

[1] Base de signatures, de comportements, etc.

[2] En termes de complétude, pertinence et précision.

4.3 Spécification des mécanismes cryptographiques[3]

Les informations relatives aux algorithmes doivent inclure :

- la description des fonctions de cryptologie offertes par le produit (chiffrement, signature, gestion des clés, etc.) ;
- la référence des algorithmes à des standards reconnus, non équivoques, et dont les détails techniques sont accessibles aisément et sans conditions, avec les paramètres et les modes opératoires de leur mise en œuvre.

Les informations relatives à la gestion des clés doivent inclure :

- la taille des clés ;
- le mode de distribution des clés ;
- le procédé de génération des clés ;
- le format de conservation des clés ;
- le format de transmission des clés.

Les informations relatives au traitement des données doivent inclure :

- la description des prétraitements subis par les données en clair avant leur chiffrement (compression, formatage, ajout d'un en-tête, etc.) ;
- la description des post-traitements des données chiffrées, après leur chiffrement (ajout d'un en-tête, formatage, mise en paquet, etc.) ;
- des sorties de référence du produit, sous format électronique, effectuées à partir d'un texte en clair et d'une clé choisis arbitrairement.

Lorsqu'un générateur de nombres aléatoires est utilisé pour la mise en œuvre de fonctions cryptographiques, la méthode et l'architecture utilisées pour ce générateur devront être décrites. Des explications seront fournies sur les raisons qui permettent de montrer que le générateur de nombres aléatoires est efficace.

Cette documentation doit répondre aux prescriptions de [CRYPTO].

5 Critères d'évaluation

Le présent chapitre fixe les critères 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.

5.1 Phase 1 - Analyse de la cible de sécurité

Tâches de l'évaluateur

Vérifier que la cible de sécurité contient les éléments décrits au chapitre 4.2 du présent document.

Vérifier que la cible n'est pas « trompeuse » et qu'elle décrit au minimum la fonctionnalité principale pour laquelle le produit est conçu.

Vérifier que les fonctions de sécurité sont pertinentes par rapport aux menaces génériques décrites dans la cible.

Vérifier qu'il n'y a pas de fonction de sécurité qui ne serait pas en lien avec une menace décrite dans la cible.

[3] Lorsque les fonctions de sécurité principales du produit sont implémentées par des mécanismes cryptographiques.

Vérifier que les mesures d'environnement sont pertinentes par rapport aux menaces et à l'usage pour lequel est prévu le produit.

De manière générale, vérifier qu'il n'y a pas d'incohérence dans la cible de sécurité.

5.2 Phase 2 – Installation du produit

Tâches de l'évaluateur

Décrire la plate-forme réellement utilisée pour réaliser les tests sur le produit. Cette plate-forme doit être représentative de l'architecture type du système d'information dans lequel le produit est normalement utilisé, dans la limite des possibilités allouées au projet d'évaluation.

Pour les produits pouvant s'installer sur plusieurs versions de système d'exploitation, indiquer le système d'exploitation utilisé et sa version, avec le maximum de précision possible (*patch*, *service pack*, etc.).

Si le produit nécessite une installation, procéder à l'installation du produit dans sa configuration typique.

Si une documentation d'installation existe, vérifier qu'elle permet d'installer le produit dans les différentes configurations couvertes par l'évaluation.

Noter toutes les informations qui permettent de mener à bien cette installation. Indiquer toutes les non-conformités par rapport à l'éventuelle documentation existante.

Noter toutes les particularités de paramétrage du système support, le cas échéant.

5.3 Phase 3 – Analyse de la conformité – analyse de la documentation

Exigences concernant le contenu et la présentation

La documentation utilisateur 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 s'assurer que son contexte d'utilisation répond aux mesures d'environnement exigées par la cible. Elle doit, à ce titre, donner les recommandations ou avertissements nécessaires vis-à-vis des différentes catégories d'utilisateurs concernés. Ces documents, par exemple les manuels de référence et les guides de l'utilisateur, doivent être structurés, avoir une cohérence interne et être compatibles avec tous les autres documents fournis à ce niveau.

La documentation d'administration doit décrire les fonctions relevant d'un administrateur, et dédiées à la sécurité. Elle doit distinguer deux types de fonctions : celles qui permettent à un administrateur de contrôler les paramètres de sécurité et celles qui lui permettent seulement d'obtenir des informations. Si un administrateur est nécessaire, elle doit décrire tous les paramètres de sécurité qui sont sous sa responsabilité. Elle doit décrire 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 caractéristiques de sécurité du produit et sur la façon dont ces caractéristiques interagissent. Elle doit décrire la façon dont le système ou le produit devra être installé et, le cas échéant, la façon dont il devra être configuré. La documentation d'administration, par exemple les manuels de référence et les guides de l'administrateur, doit être structurée, avoir une cohérence interne et être compatible avec tous les autres documents fournis à ce niveau. La documentation d'administration doit décrire comment le produit est administré de façon sûre.

Si différentes configurations sont possibles, l'impact de ces configurations sur la sécurité doit être décrit.

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 9). Ces procédures doivent garantir l'authenticité et l'intégrité du produit généré. Pendant la génération du produit, toute option ou tout changement de génération doit être audité de telle façon qu'il soit possible *a posteriori* de reconstituer exactement comment et quand le produit a été généré.

Les procédures pour assurer un démarrage et une exploitation sûrs doivent être décrites. 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. Si le produit comprend des composants matériels dédiés à la sécurité, il doit exister des fonctions de diagnostic mises en œuvre par l'administrateur ou par l'utilisateur final, ou de façon automatique, pouvant être exécutées par le produit dans son environnement d'exploitation.

Tâches de l'évaluateur

Lister les documents analysés.

Vérifier que les informations fournies satisfont les exigences concernant le contenu et la présentation, et donner un avis sur leur lisibilité et leur exhaustivité. L'évaluateur procédera par échantillonnage si la documentation est importante, en privilégiant :

- la cible de sécurité fournie par le commanditaire ;
- la documentation utilisateur ;
- la documentation d'installation, d'administration et d'exploitation ;
- les documents techniques portant sur les fonctions et mécanismes de sécurité ;
- si des fonctions essentielles du produit utilisent des mécanismes cryptographiques, la cryptographie doit être évaluée (voir §4.11).

Si tout ou partie de la documentation est indisponible, indiquer si le produit peut néanmoins être installé, 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. 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).

5.4 Phase 4 – Analyse de la conformité – revue du code source (si disponible)

Tâches de l'évaluateur

Donner un avis d'expert sur la lisibilité et la structuration du code source (exemples de critères : existence de commentaires, découpage en modules, typage des données, portabilité, etc.), en précisant les modules qui ont été regardés. Il est possible de procéder par échantillonnage.

On notera que dans le cas d'un code développé dans un cadre coopératif par de multiples développeurs, l'analyse d'un échantillon du code peut s'avérer non significatif.

5.5 Phase 5 – Analyse de la conformité – tests du produit

Tâches de l'évaluateur

Reprendre une à une les fonctionnalités de sécurité et les mécanismes cryptographiques[4] du produit et les tester.

Indiquer les tests fonctionnels ou les mécanismes mis en œuvre, en précisant :

- la fonctionnalité ou le mécanisme testé ;
- les conditions du test qui sont utiles à sa mise en œuvre (par exemple, taille et type du fichier en entrée, taille et type du fichier en sortie, analyse éventuelle du cryptogramme, etc.) ;
- les limites de la fonctionnalité le cas échéant ;
- si la fonctionnalité ou le mécanisme est conforme ou pas ;
- les éléments d'appréciation (avis d'expert).

5.6 Phase 6 - Résistance des mécanismes/fonctions

Définition

Même si elle est conforme à sa spécification, une fonction de sécurité peut être court-circuitée, désactivée, altérée, contournée ou rendue inefficace par une attaque. Une telle attaque tire généralement profit d'insuffisances dans l'implémentation du produit, sa conception, ou dans ses principes de sécurité sous-jacents. La capacité du produit à contenir une telle attaque doit donc être estimée. Il est nécessaire pour cette analyse de prendre en considération le niveau de ressources nécessaires à un attaquant pour réussir chaque attaque considérée.

Exigences concernant le contenu et la présentation

Les mécanismes étudiés sont ceux qui implémentent les fonctions de sécurité proposées par le produit, et décrites dans la cible de sécurité. Pour les mécanismes mettant en œuvre des algorithmes cryptographiques, une spécification détaillée doit être fournie.

Tâches de l'évaluateur

Le rôle de l'évaluateur est :

- d'identifier des mécanismes de sécurité implémentant les fonctions de sécurité ;
- d'analyser le fonctionnement de chaque mécanisme pour vérifier qu'il est en mesure de rendre le service voulu ;
- en cas de vulnérabilités découvertes, de proposer une cotation de l'exploitation de chaque vulnérabilité, en utilisant les tables de cotation qui suivent ;
- 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 ;
- 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.

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 seront à évaluer selon les tables de cotation du document [JIL_HW] ;

[4] Lorsque les fonctions de sécurité principales du produit sont implémentées par des mécanismes cryptographiques.

- les produits de type « équipement matériel avec boîtier sécurisé » seront à évaluer 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.

Facteur	**Valeurs**	
Temps mis pour 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[5]	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	*[6]
Type d'équipement	Aucun / standard	0

[5] Incluant le recours à de la documentation publique

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

Facteur	**Valeurs**	
nécessaire[7]	Logiciel spécialisé	2

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
20 à 24	Élevé	Non
>= 25	Très élevé	Non

5.7 Phase 7 – Analyse de vulnérabilité (intrinsèque, de construction, d'exploitation, etc.)

Tâches de l'évaluateur

Le recensement des vulnérabilités connues s'appuie sur les compétences propres de l'évaluateur et sur l'exploitation de bases de vulnérabilités. Pour ces dernières, la tâche consiste à extraire les vulnérabilités pertinentes et à vérifier si et comment elles sont exploitables sur le produit.

On distinguera deux types de vulnérabilités à traiter :

- les vulnérabilités spécifiques du produit, pour lesquelles l'analyse consiste à décrire les conditions, techniques et effets de la réalisation de la vulnérabilité, ainsi que de préciser l'existence de correctifs ou de procédures permettant de contrer, mitiger ou pallier la vulnérabilité ;
- les vulnérabilités génériques potentiellement applicables au produit. Il s'agit de vulnérabilités découvertes sur des produits similaires et pour lesquelles il n'existe pas d'information prouvant que le produit concerné s'en prémunit. La tâche d'analyse se complète alors d'une tentative – dans la limite des moyens disponibles – d'exploitation de la vulnérabilité, afin d'éprouver le produit cible.

Cette tâche consiste donc à :

a) s'assurer qu'un suivi des vulnérabilités existe pour le produit. Si le produit inclut des composants développés par un tiers (COTS ou *open source*), alors le développeur doit être informé des vulnérabilités apparaissant sur ce composant. Dans le cas où cette information n'est pas publique, il doit en informer l'évaluateur ;

b) recenser les vulnérabilités connues du produit. Pour chaque vulnérabilité, rechercher un correctif, officiel ou non, ou une méthode de contournement permettant de limiter les effets de la vulnérabilité. Lorsque le produit inclut des composants développés par un tiers, surtout lorsque ces composants sont anciens, un grand nombre de vulnérabilités publiques est susceptible d'être présent sur le produit. Cela peut rendre impossible la réalisation de

[7] 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)

l'évaluation en temps contraint. Pour cette raison, l'évaluateur est autorisé à exiger du développeur :

- une liste exhaustive des vulnérabilités publiques des composants tiers inclus dans le produit, et
- un argumentaire démontrant que ces vulnérabilités sont non-applicables, sans impacts, corrigées ou contournables ;

Cette pré-analyse effectuée par le développeur ne se substitue pas aux tâches de l'évaluateur, mais vise à les rendre réalisables dans le temps contraint de l'évaluation.

c) recenser les vulnérabilités connues pour les produits de la même catégorie. Il s'agit des vulnérabilités connues sur l'ensemble des produits de la catégorie, ainsi que des vulnérabilités théoriques potentielles ;

d) mettre en œuvre, tester et valider certaines vulnérabilités, selon des critères de choix comme la faisabilité, l'exploitabilité ou l'absence de correctif.

5.8 Phase 7bis – Analyse de vulnérabilité du système hôte

Tâches de l'évaluateur

Dans le cas où le produit nécessite des privilèges particuliers pour s'exécuter sur le système hôte, l'évaluation devra également porter sur l'impact de l'installation du produit sur la sécurité du système hôte. On entend par système hôte autant un système d'exploitation qu'un réseau. Typiquement, si le produit nécessite des privilèges d'exécution particuliers du système d'exploitation, l'évaluateur devra rechercher si le produit permet de réaliser une escalade de privilèges.

Le rôle de l'évaluateur est :

- d'identifier les privilèges ou les conditions de cloisonnement nécessaires sur le système hôte pour que le produit s'exécute correctement ;
- de donner un avis d'expert motivé sur l'impact qu'a le produit sur la sécurité de son système hôte.

5.9 Phase 8 – Analyse de la facilité d'emploi

Tâches de l'évaluateur

Identifier les cas où le produit peut donner une fausse impression de sécurité à un administrateur ou un utilisateur final.

Identifier les éventuelles fonctionnalités intrinsèquement non-sûres qu'il convient de ne pas utiliser si elles mènent ou contribuent à mener à une vulnérabilité exploitable, ou encore si la complexité de leur mise en œuvre est nuisible à la confiance dans la fiabilité de la configuration.

Fournir, lorsque cela est possible, des recommandations réalistes permettant une utilisation sûre du produit malgré ses éventuelles vulnérabilités.

5.10 Phase 9 – Entretien avec les développeurs

Tâches de l'évaluateur

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.

L'évaluateur donne un avis d'expert sur la capacité qu'a le développeur à maîtriser son produit, la sécurité de celui-ci, etc. L'évaluateur pourra s'inspirer de la liste qui suit pour étayer son avis :

- sécurité de l'environnement de développement : locaux, types de personnels, réseau de développement, etc. ;
- existence d'un système qualité ;
- existence d'une documentation de conception et de réalisation du produit ;
- existence d'une gestion de configuration ;
- capacité des développeurs à répondre aux questions posées.

5.11 Phase 10 – Évaluation de la cryptographie (si le produit implémente des mécanismes cryptographiques)

Tâches de l'évaluateur

L'évaluation de la cryptographie doit être réalisée dès lors que des fonctionnalités essentielles du produit sont implémentées par des mécanismes cryptographiques.

L'évaluateur doit pouvoir disposer d'un support technique pour interpréter les fournitures décrites au paragraphe 4.3.

La vérification de la conformité des mécanismes cryptographiques par rapport aux exigences du référentiel technique de l'ANSSI [RGS_B] se fait par une analyse documentaire.

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 ;
- 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.

Cas des générateurs de nombres aléatoires :

L'évaluateur vérifiera que l'architecture du générateur de nombres aléatoires répond aux exigences décrites dans le référentiel technique de l'ANSSI [RGS_B].

Il indiquera les éventuels tests qu'il a réalisés pour s'assurer du caractère aléatoire de la source.

6 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 augmentée » (au sens du chapitre 5.6) 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.

L'évaluateur doit proposer une cotation pour chaque fonction et mécanisme de sécurité le cas échéant décrit dans la cible de sécurité. S'il n'est pas possible d'établir cette cotation pour une ou plusieurs fonctions, l'évaluateur doit le mentionner explicitement dans son rapport (RTE) et en indiquer les raisons.

Le RTE comporte au minimum les informations suivantes :

- le rappel du contexte de l'analyse (contexte d'emploi, durée de l'analyse, menaces, etc.) ;
- une synthèse de la documentation permettant une description fonctionnelle des fonctions de sécurité ou liées à la sécurité ; ce qui est attendu fonctionnellement du produit (résumé de ses caractéristiques de sécurité notamment) ;
- l'inventaire des vulnérabilités connues (CERT-FR, bases publiques, informations du développeur) et des correctifs ;
- la liste des principaux outils d'analyse utilisés ;
- une synthèse des résultats des tests effectués sur le produit ;
- un bilan et une cotation des éventuelles vulnérabilités exploitables identifiées ;
- un bilan du produit et des préconisations d'utilisation ou de paramétrage dans le contexte d'emploi prévu permettant en particulier, de s'assurer qu'aucune vulnérabilité identifiée n'est exploitable pour un niveau inférieur ou égal à « Basique augmentée » (au sens du chapitre 5.6).

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

Le rapport technique d'évaluation élaboré par l'évaluateur, contenant et argumentant les résultats de l'évaluation, doit être présenté sous une forme acceptable pour être pris en considération par le centre de certification de l'ANSSI.

Si le RTE fait apparaître que le produit ne répond pas ou ne répond que partiellement à sa cible de sécurité et qu'il n'est pas possible d'identifier des contre-mesures environnementales réalistes pour améliorer cette situation, le produit sera considéré comme ne répondant pas à sa cible de sécurité.

Il en est de même si les tests font apparaître des dysfonctionnements du produit, n'en permettant pas un usage normal ou l'usage prévu, l'affaiblissement du système hôte ou si certaines conclusions du RTE sont « non concluantes », par exemple faute d'information.

Enfin, un verdict d'échec pourra être prononcé si le produit inclut un composant tiers ne faisant pas l'objet d'un suivi de vulnérabilités. Cela peut par exemple concerner :

- un composant en version *beta* ;
- un composant dont le développeur a abandonné la maintenance ;
- un composant COTS dont le maintien en condition de sécurité est payant, et que le développeur n'aurait pas acheté.

7 Glossaire

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 ici sont employés dans un sens conforme à leur acception courante.

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

Argumentaire de produit (*product rationale*) : description des capacités d'un produit en matière de sécurité, donnant les informations nécessaires à un acheteur potentiel pour décider si ce produit va l'aider à répondre aux objectifs de sécurité de son système.

Assurance (*assurance*) : confiance qui peut être accordée à la sécurité fournie par une cible d'évaluation.

Canal caché (*covert channel*) : utilisation d'un mécanisme non prévu pour la communication, pour transférer des informations d'une manière qui viole la sécurité.

Certification (*certification*) : délivrance d'une déclaration formelle confirmant les résultats d'une évaluation, et le fait que les critères d'évaluation utilisés ont été correctement appliqués.

Cible de sécurité, CdS, (*security target*, ST) : spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation. Elle spécifiera aussi les menaces qui pèsent sur les biens sensibles ainsi que les mécanismes de sécurité particuliers qui seront employés.

Cible d'évaluation (*target of evaluation*, TOE) : système ou produit qui est soumis à une évaluation de sécurité.

Client (*customer*) : personne ou organisme qui achète une cible d'évaluation.

Cohésion de la fonctionnalité (*binding of functionality*) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la capacité de ses fonctions et mécanismes dédiés à la sécurité à coopérer pour former un ensemble intégré et efficace.

Commanditaire (*sponsor*) : personne ou organisme qui demande une évaluation.

Confidentialité (*confidentiality*) : prévention de la divulgation non autorisée de l'information.

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 système ou 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.

Développeur (*developer*) : personne ou organisme qui fabrique une cible d'évaluation.

Disponibilité (*availability*) : prévention d'un déni non autorisé d'accès à l'information ou à des ressources.

Documentation (*documentation*) : information écrite (ou autrement enregistrée) concernant une cible d'évaluation exigée pour une évaluation. Cette information peut, mais ce n'est pas impératif, être rassemblée en un seul document constitué dans ce but.

Documentation d'administration (*administration documentation*) : information sur une cible d'évaluation fournie par le développeur à l'usage d'un administrateur.

Documentation d'exploitation (*operational documentation*) : information fournie par le développeur d'une cible d'évaluation pour spécifier et expliquer comment les clients devront l'utiliser.

Documentation utilisateur (*user documentation*) : information sur une cible d'évaluation fournie par le développeur à l'usage de ses utilisateurs finaux.

Efficacité (*effectiveness*) : 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.

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.

Estimation de la vulnérabilité (*vulnerability assessment*) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la mesure dans laquelle des vulnérabilités connues dans la cible d'évaluation pourraient compromettre en pratique sa sécurité telle qu'elle est spécifiée dans la cible de sécurité.

Evaluateur (*evaluator*) : personne ou organisme indépendant qui effectue une évaluation.

Evaluation (*evaluation*) : estimation d'un système ou d'un produit par rapport à des critères d'évaluation définis.

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.

Exigences concernant les éléments de preuve (*requirements for evidence*) : partie des critères d'évaluation pour une phase ou un aspect particulier de l'évaluation qui définit la nature des éléments de preuve destinés à montrer que les critères relatifs à cette phase ou à cet aspect sont satisfaits.

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.

Intégrité (*integrity*) : prévention d'une modification non autorisée de l'information.

Langages de programmation et compilateurs (*programming languages and compilers*) : outils de l'environnement de développement utilisés dans la construction du logiciel et/ou du microprogramme d'une cible d'évaluation.

Mécanismes de sécurité (*security mechanism*) : logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée à la sécurité ou contribuant à la sécurité.

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

Objectifs de sécurité (*security objectives*) : contribution à la sécurité qu'une cible d'évaluation est destinée à apporter.

Organisme de certification (*certification body*) : organisme national indépendant et impartial qui effectue des certifications.

Pertinence de la fonctionnalité (*suitability of functionality*) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la pertinence des fonctions et des mécanismes de sécurité de la cible d'évaluation pour réellement contrer les menaces envers la sécurité de la cible d'évaluation, identifiées dans sa cible de sécurité.

Procédure d'exploitation (*operating procedure*) : ensemble de règles définissant l'emploi correct d'une cible d'évaluation.

Procédure de réception (*acceptance procedure*) : procédure utilisée pour prendre les objets produits au cours des processus de développement, production et maintenance d'une cible d'évaluation et les placer délibérément sous le contrôle d'un système de gestion de configuration.

Produit (*product*) : paquetage logiciel et/ou matériel des technologies de l'information qui assure une fonctionnalité conçue pour être utilisée ou incorporée au sein de multiples systèmes.

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

Résistance des mécanismes (*strength of mechanism*) : aspect de l'estimation de l'efficacité d'une cible d'évaluation qui recouvre la capacité de ses mécanismes de sécurité à résister à une attaque directe contre des défauts dans les algorithmes, les principes et les propriétés sous-jacents.

Sécurité (*security*) : combinaison de confidentialité, d'intégrité, de disponibilité, d'authentification et de non-répudiation.

Spécification des besoins (*requirements*) : phase du processus de développement dans laquelle la cible de sécurité d'une cible d'évaluation est produite.

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 faire pour vérifier les informations fournies par le commanditaire de l'évaluation, et les actions complémentaires qu'il doit effectuer.

Test 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).