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 6 septembre 2018

N° 16403 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CSPN-NOTE-01/3

NOTE D'APPLICATION

METHODOLOGIE D'EVALUATION EN VUE D'UNE CERTIFICATION DE SECURITE DE PREMIER NIVEAU - CONTENU ET STRUCTURE DU RTE

Application : Dès son approbation.

Diffusion : Publique.

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

Guillaume POUPARD
[ORIGINAL SIGNE]

Suivi des modifications

Edition	Date	Modifications
Phase expérimentale	30 janvier 2008	Première rédaction pour la phase expérimentale, abrogée par la présente procédure.
1	30 mai 2011	Fin de la phase expérimentale. Changement de dénomination de l'organisme de certification (ANSSI) et améliorations de forme.
2	23 avril 2014	Modification du domaine de classification du document : passage d'une instruction à une note d'application. Retrait des redondances vis-à-vis de [CRITERES]. Mise en conformité vis-à-vis de la procédure ANSSI-CSPN-CER-P-01.
3	6 septembre 2018	Restructuration du contenu du RTE

En application du décret n° 2002-535 du 18 avril 2002 modifié, la présente 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 note d'application

La présente note d'application fixe le format et les informations attendues dans les rapports techniques d'évaluation (RTE) de certification de sécurité de premier niveau (CSPN). Elle constitue un complément à la description des critères d'évaluation CSPN décrit par [CRITERES] (voir section 2 ci-après).

Cette méthodologie peut être affinée en fonction du type de produit à évaluer. Dans ce cas, la méthodologie spécifique doit être utilisée.

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.
[CRITERES]	Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-I-02, version en vigueur.
[NOTE 18]	Prise en compte des outils dans les évaluations logicielles, référence ANSSI-CC-NOTE-18, version en vigueur.
[NOTE 20]	Règles relative à la mise en œuvre des évaluations sécuritaires, référence ANSSI-CC-NOTE-20, version en vigueur.

3. Introduction

L'évaluation d'un produit doit permettre de vérifier qu'il fournit bien les fonctions de sécurité indiquées dans sa cible de sécurité, que toutes les fonctions de sécurité atteignent au moins un niveau intrinsèque de résistance « Enhanced-Basic[1] » et qu'aucune vulnérabilité 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.

Les RTE doivent tous se conformer aux paragraphes énumérés en Annexe A. Cette annexe présuppose que le rapport soit renseigné selon l'ordre décrit ci-dessous, les deux étapes principales étant l'analyse de conformité et de résistance, et l'étude des vulnérabilités.

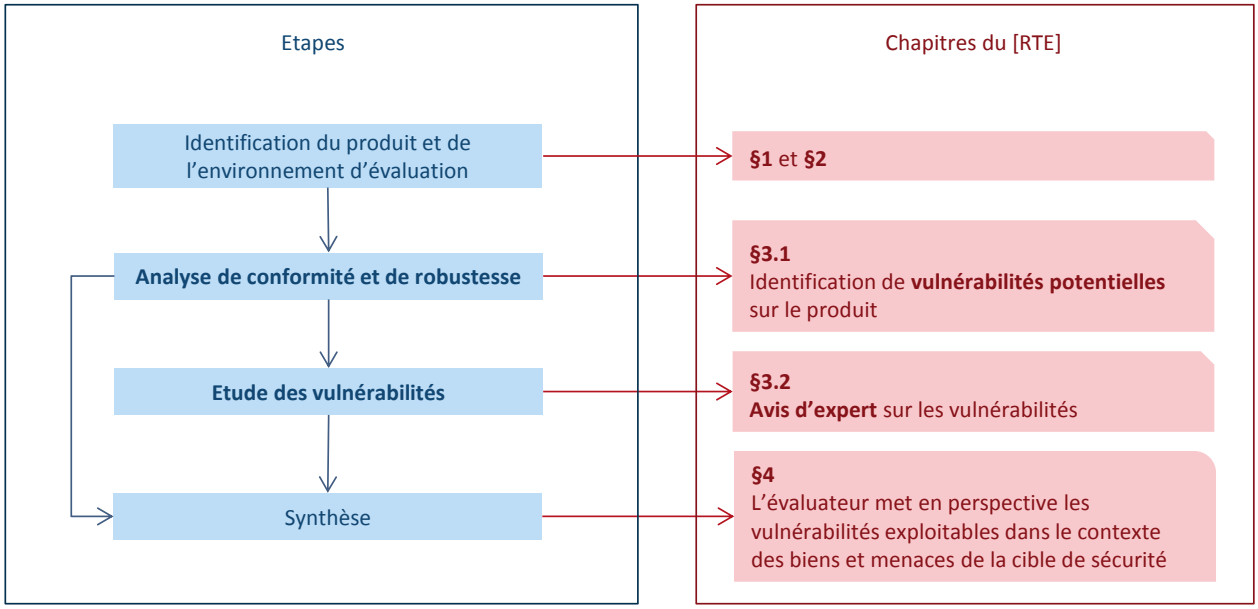

Figure 1 - Structure générale du rapport d'évaluation.

[1] Au sens de [CEM].

En conséquence, l'évaluation consiste en deux phases principales :

- l'évaluateur détecte des *vulnérabilités potentielles* sur le produit. Cette première phase inclut la plupart des phases de l'évaluation au sens du document [CRITERES], comme le décrit l'image ci-dessous.
- l'évaluateur étudie dans quelle mesure ces *vulnérabilités potentielles* sont *effectivement exploitables* sur le produit considéré. Cette phase consiste, pour l'évaluateur, à clarifier l'exploitabilité des vulnérabilités potentielles :
    - soit par une exploitation (test du produit) ;
    - soit par une cotation d'exploitation de cette vulnérabilité ;
    - soit par un argumentaire précisant pourquoi la vulnérabilité n'est pas considérée comme exploitable.

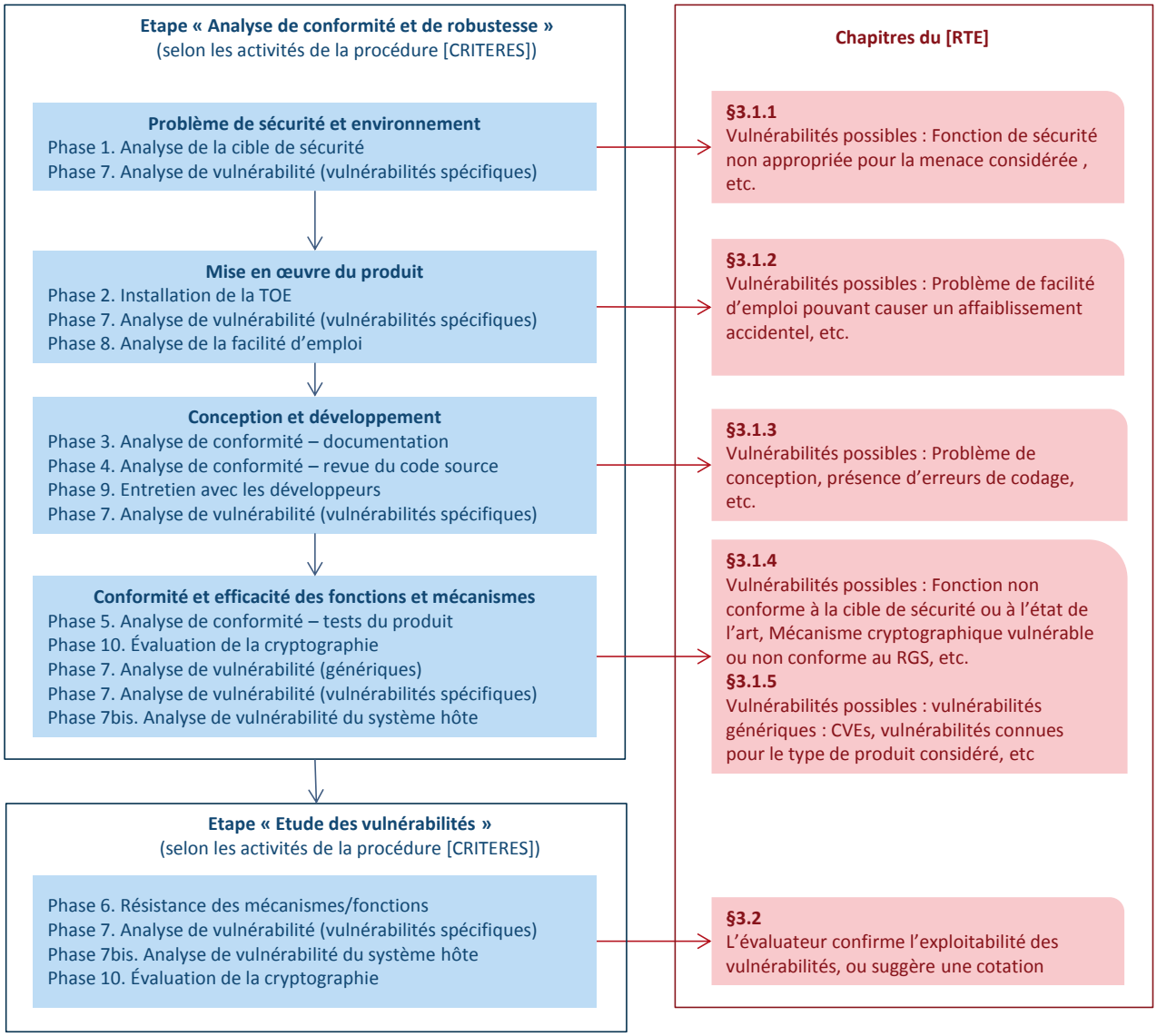

Figure 2 - Correspondance entre les phases d'évaluation décrites dans [CRITERES] et le contenu du [RTE].

L'évaluateur rédige enfin une synthèse afin de :

- mettre en lumière les vulnérabilités exploitables ou exploitées ;
- mettre en perspective ces vulnérabilités dans le contexte de la cible. Il s'attache à clarifier quels biens peuvent être compromis, et par quel chemin d'attaque.

Cette synthèse lui permet de conclure quant à l'aptitude ou non du produit à être certifié.

Annexe A : Contenu du RTE

1. Identification du rapport technique d'évaluation

Le RTE doit permettre d'identifier clairement le projet concerné, la référence et la version du RTE, ses auteurs et son circuit d'approbation. Le tableau ci-dessous est fourni en exemple. Le CESTI pourra y substituer sa propre présentation, en fonction des règles de son système qualité.

NOM DU PROJET D'EVALUATION	*Identifiant unique (référencé dans la lettre d'enregistrement)*
REFERENCE DU RTE	*Identifiant unique fourni par le CESTI*
AUTEUR(S)	*Expert(s) intervenant dans la réalisation de l'analyse*
APPROBATEUR(S)	*Nom du contrôleur technique*
DATE DE CREATION DU RTE	*Date de création du RTE*
DATE DE MISE A JOUR DU RTE	*Date de mise à jour du RTE [correspondant au N° de version du RTE]*
N° DE VERSION DU RTE	*N° de version du RTE*
DIVERS	*Texte libre*

2. Identification du produit évalué et de la cible

2.1. Références et versions de la cible d'évaluation

Le RTE doit permettre d'identifier clairement la version du produit évalué ainsi que le domaine technique concerné. Le tableau ci-dessous est fourni en exemple. Le CESTI pourra y substituer sa propre présentation, en fonction des règles de son système qualité.

Cette section identifie également la version des documents requis pour l'installation : cible de sécurité et guides du produit.

NOM DE L'EDITEUR	*Nom de l'éditeur du produit*
NOM DU PRODUIT	*Nom commercial*
NOM DE LA CIBLE D'EVALUATION	*Si différent du nom commercial*
N° DE VERSION ANALYSEE	*N° exact (version, release)*
CORRECTIFS EVENTUELS APPLIQUES	*Identifiants des correctifs éventuels appliqués*
CIBLE DE SECURITE	*Version et date de la cible de sécurité*
GUIDES	*Version et date des différents guides du produit évalué (guide d'installation, d'administration, d'utilisation…)*
DOMAINE TECHNIQUE CSPN	*Sélectionner parmi les domaines de la procédure [CSPN]*
DIVERS	*Texte libre*

2.2. Procédure d'identification du produit évalué

L'évaluateur doit décrire la procédure utilisée lors de l'évaluation pour identifier la version livrée ; si cette méthode n'est pas immédiatement accessible à l'utilisateur final, l'évaluateur décrira une procédure alternative d'identification permettant à un utilisateur final d'identifier le produit et sa version. Une capture d'écran ou photo de l'affichage de la version sera incluse. Dans le cas d'un boitier matériel, le numéro de série du boitier sera indiqué.

Si d'autres procédures permettent d'identifier le produit, l'évaluateur pourra mentionner leur existence sans nécessairement les décrire. Enfin un avis pourra être émis dans le cas d'incohérences ou imprécisions sur l'identification du produit ou de ses composants.

3. Détail des travaux d'évaluation

3.1. Analyse de conformité et de résistance

3.1.1. Problème de sécurité et environnement

L'évaluateur s'attachera à analyser les fonctionnalités, ainsi que l'environnement d'utilisation et de sécurité. Cette analyse portera sur la cible de sécurité et la documentation fournie par le développeur, ainsi que sur l'élaboration de la plate-forme de test.

3.1.1.1. Spécification de besoin et problème de sécurité

L'évaluateur ***ne complétera cette partie que si les informations fournies par le développeur sont jugées insuffisantes, inexactes ou incohérentes après analyse****. L'évaluateur précisera notamment les éléments absents ou inexacts dans la « description générale » de la cible de sécurité du produit :*

- *pour quel usage le produit a-t-il été développé ?*
- *quelles sont les menaces portant sur les biens sensibles manipulés par le produit ?*
- *quelles sont les fonctions de sécurité permettant de parer les menaces identifiées ?*

Si le contenu de la cible de sécurité est satisfaisant, l'évaluateur se contentera d'indiquer « Conforme au paragraphe Y de la cible de sécurité ».

3.1.1.2. Utilisation et environnement / Argumentaire du produit

L'évaluateur ***ne complétera cette partie que si les informations fournies par le développeur sont jugées insuffisantes, inexactes ou incohérentes après analyse****. L'évaluateur pourra notamment fournir un avis sur le positionnement indiqué dans la cible de sécurité et le reformuler (par exemple, cas d'un produit destiné au grand public mais nécessitant des connaissances avancées). Il précisera quels sont les utilisateurs typiques du produit, par exemple :*

- *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).*

L'évaluateur identifiera également:

- *la manière dont il est prévu d'utiliser ce produit ;*
- *l'environnement prévu pour son utilisation et les menaces supposées dans cet environnement.*

Si le contenu de la cible de sécurité est satisfaisant, l'évaluateur se contentera d'indiquer pour chaque sous paragraphe suivant « Conforme au paragraphe Y de la cible de sécurité ».

3.1.1.3. Avis d'expert et vulnérabilités potentielles identifiées

L'évaluateur émettra un avis sur les vulnérabilités potentielles identifiées lors de l'analyse. Ces vulnérabilités sont typiquement des problèmes de cohérence de la cible de sécurité, par exemple :

- *une hypothèse abusive au regard de l'environnement d'utilisation prévue ;*
- *une menace non prévue par la cible, mais qui nécessite d'être ajoutée au regard des biens sensibles décrits ;*

- *une fonction de sécurité non pertinente pour couvrir une menace donnée ;*
- *l'absence de fonctions de sécurité pour couvrir une menace ;*
- *etc.*

Il est recommandé de donner des identifiants[2] à ces vulnérabilités, afin de pouvoir s'y référer lors de l'étude des vulnérabilités (section 3.2) et lors de la synthèse (section 4).

3.1.2. Mise en œuvre du produit

3.1.2.1. Installation

L'évaluateur donnera les informations suivantes :

- *options d'installation retenues pour l'évaluation ;*
- *particularités de paramétrage de l'environnement ;*
- *description de l'installation (si non ou insuffisamment documentée) et des non-conformités éventuelles ;*
- *durée de l'installation ;*
- *notes et remarques diverses.*

3.1.2.2. Facilité d'emploi

L'évaluateur cherchera à identifier les cas où le produit peut être configuré ou utilisé d'une manière non sécurisée, par inattention, défaut d'information ou à cause de sa complexité de mise en œuvre. L'évaluateur s'attachera aux fonctionnalités intrinsèquement non sûres, mais également au risque qu'un utilisateur finisse par placer le produit dans une configuration non sûre en raison de la complexité d'usage du produit. Ces vulnérabilités sont typiquement des réductions non intentionnelles du niveau de sécurité causées par la complexité du produit ou une documentation insuffisante concernant :

- *son/ses processus d'installation ;*
- *ses modes d'utilisation ;*
- *les profils des utilisateur considérés ;*
- *etc.*

3.1.2.3. Avis d'expert et vulnérabilités potentielles identifiées

L'évaluateur fournira un avis sur les vulnérabilités potentielles identifiées lors de l'analyse de la facilité d'emploi.

Il est recommandé de donner des identifiants[3] à ces vulnérabilités, afin de pouvoir s'y référer lors de l'étude des vulnérabilités (section 3.2) et lors de la synthèse (section 4).

Dans le cas où de telles vulnérabilités potentielles seraient identifiées, l'évaluateur recommandera une configuration, ou des conditions de mise en œuvre, permettant d'atteindre le meilleur niveau de sécurité

[2] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Absence de chiffrement local de la donnée sensible XXX »).

[3] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Risque de mauvaises configuration des clés à l'installation »).

afin de contrer les menaces identifiées. Une réduction du périmètre fonctionnel du produit (au sens de la sécurité) peut éventuellement être proposée.

3.1.3. Conception et développement

3.1.3.1. Analyse de la documentation et des fournitures

L'évaluateur doit faire une revue complète des fournitures. En particulier, si l'évaluation est tenue de suivre une méthode particulière pour un domaine donné, l'évaluateur doit systématiquement faire la revue des fournitures requises par la méthode. Les fournitures incluent typiquement les fournitures documentaires (par exemple les guides du produit). A ces fournitures de base peuvent s'ajouter d'autres documents (par exemple issues de la conception du produit). Il peut être également nécessaire, pour un produit donné, de fournir des fournitures non documentaires : environnements de développement ou de compilation, outils ou vecteurs de test, etc.

3.1.3.2. Analyse de la spécification cryptographique

Cette partie est à renseigner uniquement si le produit implémente des mécanismes cryptographiques.

3.1.3.3. Revue du code source

Cette partie est à renseigner uniquement si le code source est disponible (ce point peut être requis par une méthode particulière pour un domaine donné).

3.1.3.4. Entretien avec les développeurs

Cette tâche est facultative. En revanche, si l'évaluateur a été amené à interagir avec le développeur dans le cadre de l'évaluation, il est tenu de décrire la nature des échanges avec le développeur, le résultat de ces échanges et, lorsqu'applicable, de donner un avis sur sa maîtrise du produit et ses processus de développement.

3.1.3.5. Avis d'expert et vulnérabilités potentielles identifiées

L'évaluateur fournira un avis sur les vulnérabilités potentielles identifiées lors de l'analyse. Ces vulnérabilités sont typiquement des failles de conception :

- *erreur de conception sécuritaire, par exemple choix d'un protocole inadapté pour le problème considéré ;*
- *utilisation de mécanismes cryptographiques vulnérables ;*
- *mécanismes a priori robustes mais mal implémentés ;*
- *erreurs de programmation identifiées lors de la revue de code ;*
- *etc.*

Il est recommandé de donner des identifiants[4] *à ces vulnérabilités, afin de pouvoir s'y référer lors de l'étude des vulnérabilités (section 3.2) et lors de la synthèse (section 4).*

[4] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Possible buffer overflow dans la classe XXX »).

3.1.4. Conformité et résistance théorique des mécanismes et fonctions

Pour la conformité de chaque fonction de sécurité analysée, l'évaluateur renseigne une ou plusieurs fiches « Analyse de conformité » (voir Annexe). Ces fiches doivent être annexées au RTE. L'évaluateur n'indique à cet endroit du rapport que les références à ces fiches.

3.1.4.1. Synthèse des fonctionnalités analysées / non analysées

Le tableau de synthèse suivant liste les fonctions de sécurité indiquées dans la cible de sécurité.

FONCTION	ANALYSEE	CONFORMITE A LA CIBLE	CONFORMITE A L'ETAT DE L'ART
Fonction A	*Valeurs possibles :* Oui / Non[5] / Partiellement *Indiquer si la fonction de sécurité a été analysée*	*Valeurs possibles :* Oui / Non / Partielle / NSP *Indiquer si la fonction est bien présente et correspond à la description faite dans la cible de sécurité.* *Dans le cas d'une non-conformité totale ou partielle, indiquer la référence de la fiche jointe en annexe.* *Indiquer le type d'analyse menée (tests, revue de code, autres)*	*Valeurs possibles :* [référence : conforme / non conforme / partielle[6]] / Non applicable[7] *Quand cela est pertinent, indiquer si les mécanismes mis en œuvre sont conformes à des standards ou des recommandations de référentiels existants.* *Dans le cas d'une fonction s'appuyant sur des mécanismes cryptographiques, l'évaluateur indiquera ici la conformité au RGS.*

3.1.4.2. Détails des travaux d'analyse de la conformité des fonctions de sécurité

L'évaluateur précisera les résultats de l'analyse de conformité, en particulier lorsque des fonctions n'ont pas pu être analysées ou ne l'ont été que partiellement, et comment a été réalisée cette analyse (analyse statique ou dynamique).

Des fiches de test telles que détaillées dans l'Annexe B: Modèle de fiche d'analyse de conformité des fonctions de sécurité seront rédigées pour chaque fonction effectivement testée ; elles seront de préférence placées en annexe du rapport d'évaluation et référencées dans cette section.

Il est à noter que si des tests ne sont pas possibles, d'autres moyens de vérification peuvent être utilisés par l'évaluateur (par exemple revue de code source si disponible).

[5] Si une fonction est non analysée, le verdict de l'évaluation sera nécessairement un échec. Cela peut être le cas lorsque certains dysfonctionnements du produit ne permettent pas du tout à l'évaluateur de tester certaines fonctions.

[6] La non-conformité partielle concernera typiquement les cas « tangents », par exemple lorsqu'une fonction de protection des communication utilisant du TLS est conforme à la cible de sécurité, et permet d'utiliser à la fois des *cipher suites* conformes au RGS et des *cipher suites* non conformes.

[7] Par exemple, des fonctions de contrôle d'accès ou de journalisation n'ont pas nécessairement d'état de l'art applicable.

Cette partie est de préférence structurée par fonction ; l'analyse cryptographique peut être intégrée aux fonctions, ou bien rédigée à part (par exemple si les mécanismes cryptographiques sont utilisés dans plusieurs fonctions différentes).

3.1.4.3.Avis d'expert et vulnérabilités potentielles identifiées

L'évaluateur fournira un avis sur les vulnérabilités potentielles identifiées lors de l'analyse. Ces vulnérabilités sont liées:

- *à une fonction de sécurité non conforme à sa spécification dans la cible,*
- *à une faille résultant de l'écart à une bonne pratique ou un standard,*
- *à des vulnérabilités permettant de contourner les fonctions de sécurité : canaux cachés, exploitation de données résiduelles ;*
- *etc.*

Il est recommandé de donner des identifiants[8] à ces vulnérabilités, afin de pouvoir s'y référer lors de l'étude des vulnérabilités (section 3.2) et lors de la synthèse (section 4).

3.1.5. Identification des vulnérabilités génériques

3.1.5.1.Référentiels utilisés pour l'analyse

L'évaluateur indiquera quels référentiels il a utilisé pour mener la recherche des vulnérabilités génériques.

3.1.5.2.Avis d'expert et vulnérabilités potentielles identifiées

L'évaluateur fournira un avis sur les vulnérabilités potentielles identifiées lors de l'analyse. Ces vulnérabilités sont:

- *les vulnérabilités connues ou potentielles à la sous-catégorie ;*
- *les vulnérabilités liées à l'architecture et/ou au langage utilisé ;*
- *les vulnérabilités liées à la gamme de produit concernée ;*
- *etc.*

Il est recommandé de donner des identifiants[9] à ces vulnérabilités, afin de pouvoir s'y référer lors de l'étude des vulnérabilités (section 3.2) et lors de la synthèse (section 4).

[8] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Négociation d'une *cipher suite* interdite sur protocole XXX »).

[9] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « CVE XXX – exécution de code arbitraire »).

3.2. Etude des vulnérabilités

L'objectif de ce chapitre est de donner un avis d'expert sur les vulnérabilités identifiées dans le chapitre précédent :

- *les vulnérabilités potentielles liées aux mécanismes de sécurité implémentés, non connues des bases utilisées, découvertes lors de l'analyse de résistance théorique, par exemple :*
    - *fonction de sécurité non appropriée pour la menace considérée (voir 3.1.1) ;*
    - *problème de facilité d'emploi pouvant causer un affaiblissement accidentel de la fonction (voir 3.1.2) ;*
    - *problème de conception menant à un défaut de sécurité ou fonction mettant en œuvre un mécanisme cryptographique vulnérable (voir 3.1.3) ;*
    - *fonction non conforme à la cible de sécurité, mécanisme cryptographique non conforme au RGS, existence d'une vulnérabilité permettant d'affaiblir, contourner ou désactiver la fonction (voir 3.1.4) ;*
    - *etc.*
- *les vulnérabilités génériques (voir 3.1.5)*
    - *vulnérabilités connues ou potentielles à la sous-catégorie ;*
    - *vulnérabilités liées à l'architecture et/ou au langage utilisé ;*
    - *vulnérabilités liées à la gamme de produit concernée ;*
    - *etc.*

L'évaluateur ne s'attachera pas uniquement aux vulnérabilités touchant au produit, mais également aux vulnérabilités sur la sécurité du système hôte pouvant découler de l'utilisation du produit, en particulier quand cette utilisation nécessite des privilèges particuliers sur le système hôte. Il s'agit aussi de donner un avis sur l'impact d'un point de vue sécurité du produit sur le système d'information dans lequel il est déployé.

Si des outils ou des méthodologies spécifiques sont nécessaires pour l'exploitation de la vulnérabilité, ils seront décrits. Si l'évaluateur doit utiliser des outils fournis par le développeur ou un tiers, ils seront livrés avec le produit dans la mesure où ils sont libres de droits (logiciels libres ou développés sur mesure au titre du marché). L'évaluateur doit dans ce cas effectuer une phase de validation des outils, et préciser dans le RTE ce qui a été effectué lors de cette phase. Cette phase doit notamment être effectuée en conformité avec la [NOTE 18].

VULNERABILITE	EXPLOITATION (EXPLOITEE / NON EXPLOITABLE / EXPLOITABLE / RESIDUELLE)
#ID_VULN	Indiquer si la vulnérabilité est **exploitée**, **non exploitable**, **exploitable** ou **résiduelle**. Un diagramme, dans l'Annexe C: Classification des vulnérabilités, précise la démarche permettant de classifier les vulnérabilités selon ces catégories. Selon le cas, l'évaluateur sera amené à faire une cotation de la vulnérabilité : - **Vulnérabilités Exploitées** (l'évaluateur a pu mettre en œuvre la vulnérabilité avec succès) : Le détail des opérations menées doit être jointe au rapport (enregistrement des résultats et des moyens utilisés). La cotation de l'attaque n'est nécessaire que : o si l'évaluateur considère qu'il était dans un cas excessivement favorable, rendant l'exploitation non représentative d'un attaquant de type Enhanced-Basic (par exemple accès au code source, utilisation d'outils perfectionnés, etc) ; o sur demande de l'ANSSI. - **Vulnérabilités exploitables (**non directement mises en œuvre, mais estimées possibles pour un attaquant Enhanced-Basic ou inférieur) : l'évaluateur doit s'appuyer sur une cotation[10] ; - **Vulnérabilités non exploitables (**ne peuvent pas être mises en œuvre dans le contexte d'usage prévu[11], notamment en raison des hypothèses sur le produit) : un argumentaire est requis de la part de l'évaluateur mais il n'est pas nécessaire de faire une cotation (voir Annexe C pour plus de détails) ; - **Vulnérabilités résiduelles** : l'évaluateur doit s'appuyer sur une cotation[12] (voir Annexe C pour plus de détails).

3.2.1. Vulnérabilité #ID_VULN

*Pour chacune des vulnérabilités **#ID_VULN** identifiées, l'évaluateur précisera :*

- *le scénario d'exploitation, dans le cas où l'évaluateur a réussi à exploiter la vulnérabilité ;*
- *le chemin d'attaque identifié : l'évaluateur doit préciser si celui-ci met en défaut une ou plusieurs fonctions de sécurité et/ou quels mécanismes ont été mis en défaut ;*
- *les prérequis pour l'exploitation ;*
- *la cotation (si nécessaire) ;*
- *éventuellement, les hypothèses rendant la vulnérabilité non exploitable ou résiduelle.*

[10] La cotation est à effectuer selon la méthode définie par [CEM].

[11] Le contexte d'usage est principalement défini par les hypothèses de la cible de sécurité. Conformément à [CRITERES], il est possible de définir des *contre-mesures environnementales réalistes* permettant de remédier à certaines vulnérabilités. Dans ce cas, le développeur doit mettre à jour les guides du produit pour signaler ces contremesures à l'utilisateur. La vulnérabilité concernée sera alors déclarée comme *non exploitable*.

[12] La cotation est à effectuer selon la méthode définie par [CEM].

4. Synthèse de l'évaluation

4.1. Synthèse de la sécurité du produit

Ce chapitre vise à fournir une synthèse générale de la sécurité du produit. Cette synthèse condense l'ensemble des travaux décrits dans le chapitre 3 et les met en perspective par rapport au problème de sécurité défini dans la cible. L'évaluateur renseignera le tableau ci-après.

Chaque ligne correspond à une menace issue de la cible de sécurité, ou une menace identifiée par l'évaluateur mais non décrite dans la cible de sécurité (voir chapitre 3.1.1), ou encore une menace de non-innocuité, c'est-à-dire un risque causé par le produit évalué sur son environnement. Alternativement aux menaces, l'évaluateur peut choisir de structurer cette présentation en fonction des biens sensibles identifiés par le cible de sécurité.

Si les vulnérabilités identifiées suggèrent plusieurs chemins d'attaque pour un même type de menace, il est conseillé de créer plusieurs lignes pour une même menace.

BIENS OU MENACES[13]	CHEMIN D'ATTAQUE	EXPLOITABILITE
Bien ou Menace 1 *(cible)*	*Si un chemin d'attaque existe, décrire ce chemin en mettant en œuvre les vulnérabilités du produit décrites dans le chapitre 3.2.* *Dans le cas contraire, indiquer « pas de chemin d'attaque »*	*Les vulnérabilités mises en œuvre doivent être décrites au chapitre 3.2 comme **Exploitées** ou **Exploitables.** Si l'évaluateur considère que le chemin d'attaque complet n'est pas exploitable, l'argumentaire s'appuiera sur la cotation des vulnérabilités correspondantes.*
…	…	…
***Bien ou Menace* n** *(cible)*	*id*	*id*
Bien ou Menace m *(non défini dans la cible)*	*id*	*id*
Non-innocuité du produit	*id*	*id*

4.2. Durée des travaux

PHASE	DUREE DES TRAVAUX (EN JOURS*H)

[13] L'évaluateur peut choisir de structurer le tableau selon les biens ou les menaces, et est invité à privilégier la clarté de l'explication.

PHASE	DUREE DES TRAVAUX (EN JOURS*H)
Analyse du besoin et de l'environnement	
Analyse de la mise en œuvre	
Analyse de la conception/développement	
Conformité et résistance - Analyse de la conformité, résistance et vulnérabilités	
Conformité et résistance - Analyse de la cryptographie	
Exploitation des résultats	
Synthèse et rédaction du rapport	

4.3. Avis d'expert

L'évaluateur doit indiquer si selon lui, le produit est un bon ou mauvais candidat à la certification CSPN, et motiver son choix en cohérence avec les chemins d'attaque décrits dans le chapitre 4.1 ; le produit sera considéré comme ne répondant pas à sa cible de sécurité :

- *si 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[14] ;*
- *si les tests font apparaître des dysfonctionnements du produit, n'en permettant pas un usage normal ou l'usage prévu ;*
- *si les tests montrent que le produit cause l'affaiblissement de l'environnement hôte ;*
- *si certaines conclusions du RTE sont « non concluantes », par exemple faute d'information[15].*

L'évaluateur peut utiliser ce chapitre pour donner un avis au format libre sur le produit. Par exemple, l'évaluateur peut décrire ici les réserves éventuelles qu'il a vis-à-vis du produit, indépendamment des vulnérabilités qu'il contient.

En particulier, si l'analyse du code source a révélé de nombreux problèmes potentiels liés, par exemple, à des erreurs d'implémentation telles que l'utilisation de fonctions dépréciées et/ou de constructions jugées dangereuses, l'évaluateur n'aura pu dans le temps imparti en tester effectivement qu'un échantillon. Il est dans ce cas invité à appuyer son avis sur la probabilité que de telles vulnérabilités puissent, en dépit des résultats bruts de l'évaluation, être exploitées sur le terrain.

4.4. Notes et remarques diverses

4.5. [Chapitres optionnels]

L'évaluateur est libre d'ajouter des sous-chapitres à la synthèse, tant qu'ils n'entrent pas en conflit avec les sous-chapitres imposés par le modèle. Par exemple, l'évaluateur peut ajouter :

- *un sous-chapitre traitant des « points positifs » relevés sur le produit ;*

[14] C'est notamment le cas s'il existe un chemin d'attaque exploitable menant à la compromission d'un bien sensible identifié dans la cible de sécurité.

[15] Ce type de situation est cependant une exception. La [NOTE 20] rappelle que le CESTI est autorisé à refuser les éléments de preuve fournis par le commanditaire s'ils ne permettent pas de réaliser les tâches d'évaluation dans les conditions prévues dans le dossier d'évaluation. En conséquence, un RTE aux conclusions « non concluantes » peut potentiellement donner lieu à un écart d'agrément pour le CESTI en question.

- *un sous-chapitre traitant de la gestion de projet ;*
- *etc.*

Annexe B : Modèle de fiche d'analyse de conformité des fonctions de sécurité

Fiche vierge

<table>
<tr><td colspan="2">OBJECTIF DE L'ANALYSE</td><td colspan="2">Référence Produit (et numéro de série du boitier dans le cas d'un boitier type Appliance)</td></tr>
<tr><td colspan="2" rowspan="2">Fonction de sécurité :</td><td>Réf. de la fiche</td><td>Auteur</td></tr>
<tr><td colspan="2">Objet du test :</td></tr>
<tr><td colspan="4">Scénario du test :</td></tr>
<tr><td>OPERATIONS A EFFECTUER</td><td>RESULTATS ATTENDUS</td><td colspan="2">RESULTATS OBSERVES</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="4">CONCLUSION :</td></tr>
<tr><td colspan="4"></td></tr>
</table>

Exemple

<table>
<tr><td colspan="2">OBJECTIF DE L'ANALYSE</td><td colspan="2">Logiciel PPP version 3.5</td></tr>
<tr><td colspan="2" rowspan="2">Fonction de sécurité : filtrage IP</td><td>Réf. : Test-PPP-1</td><td>Auteur : XXXXX</td></tr>
<tr><td colspan="2">Objet du test : Un pare-feu devrait re jeter tout le trafic non explicitement autorisé. Ce test vérifie que le logiciel PPP est bien dans ce cas.</td></tr>
<tr><td colspan="4">Scénario du test : machine tout juste installée</td></tr>
<tr><td>OPERATIONS A EFFECTUER</td><td>RESULTATS ATTENDUS</td><td colspan="2">RESULTATS OBSERVES</td></tr>
<tr><td>Désactiver la règle de rejet par défaut et faire un «scan» du réseau interne avec par exemple netwox 67 --ips 10.2.0.1-10.2.0.2 --ports 20-55 pour TCP et la même chose pour UDP avec la commande n° 69. Réactiver la règle.</td><td>Aucune connexion TCP ne réussit. Pour UDP, seul le port 53 doit être accessible.</td><td colspan="2">Le «scan» TCP déclare toutes les tentatives en «timeout», sauf pour le port autorisé correspondant à SMTP. Le «scan» UDP déclare «timeout» pour tous y compris le port 53 correspondant au DNS, ce qui est inattendu.</td></tr>
<tr><td colspan="4">CONCLUSION :</td></tr>
<tr><td colspan="4">Résultats corrects, le rejet du paquet UDP vers le port 53 étant dû, d'après le journal du firewall, au fait que celui-ci n'est pas un paquet DNS correct.</td></tr>
</table>

Annexe C : Classification des vulnérabilités

La figure ci-après décrit la méthode de classification des vulnérabilités.

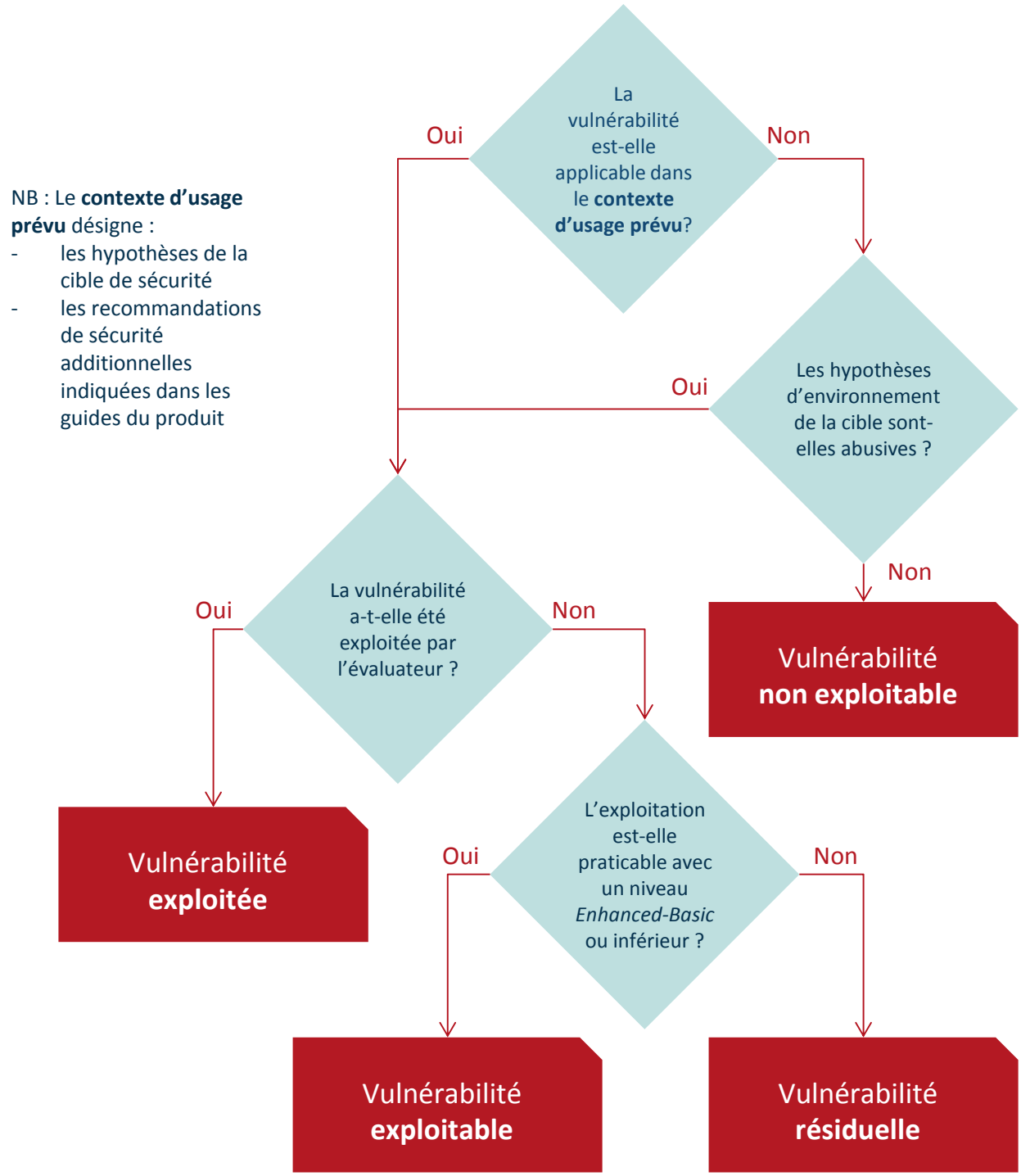

Figure 3 : Classification des vulnérabilités