PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Paris, le 12 janvier 2023

N° **45 /ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CSPN-CER-P-01_v5.0**

PROCEDURE

CERTIFICATION DE SECURITE DE PREMIER NIVEAU DES PRODUITS DES TECHNOLOGIES DE L'INFORMATION

Application **:** Dès son approbation

Diffusion **:** Publique.

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

Renaud LABELLE
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
Phase expérimentale	25 avril 2008	Première rédaction pour la phase expérimentale, diffusée sous le n° 915 SGDN/DCSSI/SDR du 25 avril 2008, et abrogée par la présente procédure.
1.0	30 mai 2011	Fin de la phase expérimentale. Passage de la charge contrainte pour l'évaluation de base (hors cryptographie) de 20h.j. à 25h.j. Changement de dénomination de l'organisme de certification (ANSSI) et améliorations de forme.
1.1	7 avril 2014	Ajout du statut d'observateur dans l'évaluation. Ajout de la possibilité de méthodologies annexes. Ajout des catégories de produit STB et environnement d'exécution sécurisé. Ajout du cas des produits nécessitant des privilèges d'exécution particuliers. Limitation de la démarche d'évaluation CSPN pour les produits disposant de certificats reconnus par l'ANSSI.
2.0	6 septembre 2018	Flexibilité de la charge d'évaluation.
2.1	13 janvier 2020	Le rapport de certification ne contient pas une cotation de la résistance des mécanismes de sécurité comme mentionné au dans la version précédente.
3.0	12 avril 2021	Suppression de la surveillance qui n'est pas utilisée en CSPN. Le choix des commanditaires se porte vers la réévaluation. Ajout de l'usage de la marque « TI SECURITE CERTIFICATION ». Ajout de la suspension et du retrait du certificat. Ajout de l'appel de la décision. Utilisation de la nouvelle charte graphique.
4.0	3 mars 2022	Ajout de la validité des certificats. Précisions apportées sur la livraison des fournitures et de leur modification.
5.0	12 janvier 2023	Ajout d'exigences relatives à l'éligibilité des produits à la certification. Passage de la limite de charge maximale à 60 hommes.jours, conformément à ANSSI-CSPN-NOTE-03.

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 évaluations 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.ssi.gouv.fr).

TABLE DES MATIERES

1 Objet de la procédure

La présente procédure décrit l'ensemble du processus de certification de sécurité de premier niveau (CSPN) d'un produit, depuis la demande officielle par un commanditaire jusqu'à l'attribution d'un certificat pour le produit évalué, ainsi que le rôle de chacun des acteurs.

2 Contexte

Le décret n° 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information définit le cadre réglementaire du schéma français d'évaluation et de certification.

Ce schéma définit l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance d'un certificat attestant qu'un produit ou un système répond aux exigences de sécurité listées dans sa cible de sécurité.

La certification de sécurité de premier niveau permet d'attester que le produit a subi avec succès une évaluation de sécurité par un centre d'évaluation agréé par l'ANSSI, l'évaluation ayant pour caractéristiques principales :

- d'analyser la conformité du produit à ses spécifications de sécurité ;
- de mesurer l'efficacité des fonctions de sécurité ;
- d'être conduite en temps et en ressources humaines (charge) contraints.

3 Définitions

Centre d'évaluation	Organisme, agréé par l'ANSSI, qui réalise l'évaluation de la sécurité du produit en vue de la CSPN.
Cible d'évaluation	Produit réel soumis à l'évaluation.
Cible de sécurité (CdS)	Document décrivant les fonctions de sécurité du produit qui font l'objet de l'évaluation et de la certification.
Commanditaire	Le commanditaire est celui qui demande la certification à l'ANSSI et qui finance la prestation d'évaluation.
CSPN	Certificat de sécurité de premier niveau (ou certification de sécurité de premier niveau, selon le contexte).
Développeur	Le terme développeur désigne l'organisation qui spécifie, élabore, ou maintient le produit ou certains de ses composants.
Observateur	L'observateur est un acteur concerné par les résultats de l'évaluation. En général, il s'agit d'un donneur d'ordre ou d'un utilisateur du produit évalué.
Rapport de certification	Rapport synthétique établi par l'ANSSI sur la base du rapport technique d'évaluation
Rapport technique d'évaluation (RTE)	Rapport établi par le centre d'évaluation, consignant les résultats de son évaluation.
TOE	Objet de l'évaluation (Target Of Evaluation)

4 Les acteurs

4.1 Liste des acteurs

Les acteurs du processus de certification sont :

- le commanditaire ;
- le centre d'évaluation ;
- le centre de certification de l'ANSSI ;
- éventuellement, le développeur du produit soumis à l'évaluation ;

- éventuellement, un (ou des) observateur(s) concerné(s) par les résultats de l'évaluation.

4.2 Le commanditaire

Le commanditaire fournit le produit, sa cible de sécurité et sa documentation. Lorsque des fonctions de sécurité essentielles du produit reposent sur des mécanismes cryptographiques, le commanditaire fournit également la documentation décrivant ces mécanismes, telle que prévue par le document [CRY-P-01].

Il fournit également le code source nécessaire lorsqu'il est exigé pour pouvoir réaliser l'évaluation conformément aux méthodes génériques et spécifiques d'évaluation.

Il passe un contrat avec un centre d'évaluation agréé par l'ANSSI pour réaliser l'évaluation de sécurité.

Il demande la certification à l'ANSSI au moyen du dossier de demande d'évaluation [DOSSIER_EVAL].

Il est destinataire du rapport technique d'évaluation (RTE) dans sa version finale validée par l'ANSSI.

Il décide de la publication ou non du rapport de certification établi par l'ANSSI.

4.3 Le centre d'évaluation

Le centre d'évaluation est agréé pour les domaines techniques dans lesquels ses compétences ont été estimées suffisantes par l'ANSSI. Un centre d'évaluation ne peut évaluer des produits en vue d'une CSPN que dans les domaines techniques pour lesquels il a été agréé. Toutefois, plusieurs centres d'évaluation peuvent associer leurs compétences afin de couvrir l'intégralité des compétences nécessaires pour évaluer un produit.

Il passe un contrat avec le commanditaire en vue de réaliser l'évaluation d'un produit dans le domaine technique pour lequel il est agréé.

Il réalise l'évaluation du produit en suivant les critères et les méthodologies élaborés par l'ANSSI en vue de la CSPN.

Il consigne les résultats de son évaluation dans un rapport technique d'évaluation (RTE), qu'il envoie à l'ANSSI pour validation.

Le centre d'évaluation et son personnel ont une obligation de secret professionnel sur les produits qu'ils évaluent et les résultats qu'ils obtiennent durant l'évaluation.

La liste des centres d'évaluation agréés pour la CSPN est tenue à jour sur le site de l'ANSSI (www.ssi.gouv.fr).

4.4 Le centre de certification de l'ANSSI

Le centre de certification de l'ANSSI élabore les critères et la méthode générique d'évaluation pour la CSPN, ainsi que des méthodes spécifiques à certains types de produits.

Il rédige les procédures, formulaires, guides et tout autre document nécessaires à la mise en œuvre la CSPN, parmi lesquels notamment :

- la procédure d'agrément des centres d'évaluation ;
- les modèles pour la rédaction des cibles de sécurité, des rapports techniques d'évaluation et des rapports de certification ;
- le formulaire de demande de CSPN.

Il s'assure que les centres d'évaluation satisfont les critères énumérés dans la procédure d'agrément des centres d'évaluation (voir [AGREMENT]) et propose leur agrément.

Il analyse les dossiers de demande de certification (cible de sécurité, durée des tests, etc.) et autorise ou non le lancement de l'évaluation.

Il valide les RTE élaborés par les centres d'évaluation avant transmission au commanditaire.

Il propose la suite à donner à chaque évaluation (certification ou non).

Il établit le rapport de certification et le certificat.

Avec l'accord du commanditaire, il fait publier la cible de sécurité et le rapport de certification des produits ayant obtenu une CSPN sur le site de l'ANSSI (www.ssi.gouv.fr).

4.5 Le développeur

Le développeur est responsable de l'élaboration éventuelle des fournitures ainsi que de l'assistance technique aux évaluateurs si nécessaire (formation, passage de tests, mise à disposition d'une plate-forme d'évaluation). Il est responsable de la protection de son savoir-faire et de ses fournitures.

4.6 L'observateur

Le commanditaire peut proposer la présence d'un observateur qui est associé au suivi de l'évaluation. L'observateur est soumis à l'acceptation de l'ANSSI.

Les observateurs sont des acteurs qui ont un intérêt particulier vis-à-vis des résultats de l'évaluation ou de son déroulement. Il s'agit en général de donneurs d'ordres qui imposent l'évaluation pour autoriser l'acquisition de produits par leur organisation ou les organisations qu'ils représentent ; il peut s'agir de gestionnaires de risques de ces organisations qui ont un intérêt particulier pour les résultats concrets de l'évaluation (par exemple, connaissance des risques résiduels), etc.

L'observateur est tenu informé du démarrage de l'évaluation ainsi que des résultats obtenus.

Les éléments précis auxquels auront accès le ou les observateurs (par exemple, le rapport technique d'évaluation ou une version allégée de ce rapport) seront déterminés avec le centre de certification, le centre d'évaluation et le commanditaire.

5 Préparation d'une demande de certification

Avant de formuler une demande de CSPN pour un produit, le commanditaire doit s'assurer :

- qu'il dispose d'une **cible de sécurité** pour le produit contenant au minimum :
  - le nom commercial du produit et une référence permettant d'identifier sans ambiguïté le produit et la version soumise à l'évaluation ;
  - une présentation du produit, décrivant clairement :
    - l'usage pour lequel le produit a été conçu, par qui et dans quel contexte d'emploi il est censé être utilisé,
    - l'environnement technique du produit (modèle d'ordinateur, système d'exploitation, etc.),
    - l'environnement organisationnel du produit (locaux sécurisés, mesures de filtrage de sécurité des administrateurs du produit, etc.),
    - le problème de sécurité auquel répond l'évaluation du produit :
      - les biens sensibles que le produit doit protéger[1],
      - les attaquants considérés (attaquant local et/ou à distance, utilisant des moyens logiciels et/ou matériels)
      - les scénarios de menaces contre lesquelles le produit offre une protection,
    - les fonctions implémentées par le produit, qui peuvent être de trois types :
      - les fonctions de sécurité évaluées permettent de parer les menaces identifiées dans la cible. Ces fonctions sont évaluées en conformité et en efficacité ;
      - les fonctions non évaluées (c'est-à-dire toutes les autres fonctions actives et accessibles sur la TOE) : la conformité de ces fonctions n'est pas évaluée lors de la CSPN, mais l'évaluation les prend en compte en tant que vecteurs d'attaque potentiels sur la TOE ;

[1] Parmi les biens sensibles, la cible devra systématiquement inclure le système hôte. En effet, l'évaluation devra systématiquement démontrer que la TOE n'induit pas de menaces sur le système hôte. Par exemple :

- Si la TOE est une application : qu'elle ne peut être utilisée pour élever ses privilèges sur le système d'exploitation sous-jacent ;
- Si la TOE est un équipement réseau : qu'elle ne peut être utilisée pour rebondir ou attaquer un autre équipement situé sur le réseau.

        - les fonctions désactivées et/ou non accessibles à un attaquant ;
    - la liste des composants tiers utilisés par la TOE (COTS et open source), ainsi que leurs versions (cette liste détaillée pourra être supprimée de la cible publique).
- qu'il respecte les exigences de [CRY-P-01], si des fonctions de sécurité essentielles du produit reposent sur des mécanismes cryptographiques ;
- que le produit est éligible à la certification CSPN (voir ANNEXE B)
- que le centre d'évaluation pourra disposer d'un accès
    - au produit ;
    - à des équipements de test si ceux-ci sont spécifiques ou dédiés ;
    - à une documentation permettant à un utilisateur final d'utiliser le produit de façon sûre (documentation utilisateur, éventuellement d'administration et d'installation) ;
- qu'aucune certification Critères Communs entrant dans le cadre des accords de reconnaissance mutuelle CCRA ou SOGIS n'est en cours ou n'a eu lieu sur une version similaire du produit[1].

6 Choix d'un centre d'évaluation

Le commanditaire passe un contrat avec un centre d'évaluation agréé (ou une association de centres d'évaluation agréés) pour le ou les domaines techniques dans lesquels est classé le produit à évaluer.

7 Demande de certification

Le commanditaire rédige et transmet au centre de certification :

- le dossier de certification (voir [DOSSIER_EVAL]) ;
- la cible de sécurité du produit ;
- le cas échéant, la documentation sur les mécanismes cryptographiques (voir [CRY-P-01]).

Si les documents ci-dessus sont modifiés après l'enregistrement du projet, le commanditaire doit prévenir et transmettre les documents modifiés au centre de certification en même temps qu'au centre d'évaluation.

8 Analyse de la demande

Le centre de certification analyse la demande et la cible de sécurité du produit. Après acceptation de ces éléments par le centre de certification, le projet de certification est enregistré et les acteurs (commanditaire, centre d'évaluation) sont avertis du démarrage du projet par un courrier de l'ANSSI.

Plusieurs raisons peuvent justifier un refus du dossier, notamment :

- dossier de demande incomplet (demande, cible de sécurité, refus d'un des engagements demandés par le formulaire de demande[2]…) ;
- centre d'évaluation non agréé ou non compétent pour le domaine technique du produit[3] ;
- non-respect des prérequis identifiés au chapitre 5, notamment produit non éligible à la CSPN.

[1] La demande de CSPN pourra être validée si l'évaluation du produit correspond à un besoin particulier que le commanditaire devra justifier dans sa demande, l'ANSSI appréciera l'opportunité et la pertinence de cette justification.

[2] Par exemple, refus du commanditaire d'informer le centre de certification sur les vulnérabilités potentielles du produit.

[3] Par exemple, si un produit réseau est implémenté dans une technologie inhabituelle pour le CESTI (par exemple FPGA), son évaluation au sens de la CSPN nécessitera non seulement des compétences réseau, mais également des compétences FPGA (il appartient à l'expert FPGA de confirmer si cette technologie induit des attaques réalisables dans les conditions définies par la cible)

9 Déroulement de l'évaluation

9.1 Livraisons des fournitures

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation. En complément à la liste des fournitures indiquée au chapitre 5, il doit diffuser la documentation utilisateur qui permet aux utilisateurs de mettre en œuvre de façon sûre les fonctions de sécurité évaluées (voir [CRITERES]/phase 3).

Toutes les fournitures sont, par défaut, envoyées au centre d'évaluation et au certificateur en charge du projet.

Si le commanditaire n'est pas le concepteur du produit ou du système, les fournitures peuvent être livrées directement par une tierce partie (par exemple un développeur ou un sous-traitant) afin de respecter la confidentialité du savoir-faire.

Aucune mise à jour documentaire n'est permise dans le cadre des évaluations CSPN sauf accord explicite du centre de certification (voir plus bas).

9.2 Généralités sur la procédure d'évaluation

L'évaluation se déroule dans un cadre méthodologique formalisé (voir [CRITERES] et [METHODE]) afin d'en garantir l'objectivité et de favoriser l'homogénéité des résultats entre les différents centres d'évaluation. Ce cadre méthodologique permet également de faciliter la comparaison des résultats des évaluations de produits similaires lorsqu'elles sont réalisées par des centres d'évaluation différents. Pour certains types de produits, une méthodologie spécifique peut exister[2]. Dans ce cas, c'est cette méthodologie qui doit être utilisée par l'évaluateur.

L'ANSSI peut demander à participer à tout ou partie des tâches d'évaluation réalisées par le centre d'évaluation.

En cas de dépassement du délai prévu pour l'évaluation, l'ANSSI peut décider de clore le projet de certification. Pour autant, le commanditaire n'est pas libéré de ses éventuelles obligations contractuelles vis-à-vis du centre d'évaluation.

Le but de l'évaluation est d'apprécier, en temps et charge contraints :

- la conformité du produit à sa cible de sécurité (§ 9.4) ;
- l'efficacité des fonctions de sécurité (§ 9.5) ;
- l'impact du produit sur la sécurité du système hôte (§9.5).

Le déroulement en temps et en charge implique entre autres conséquences :

- de fonctionner en « mode tunnel » :
    - le commanditaire n'interagit pas avec le centre d'évaluation pendant les travaux d'évaluation, sauf à la demande explicite de ce dernier ;
    - les résultats d'évaluation obtenus ne sont pas transmis au commanditaire ou développeur tant qu'ils ne sont pas validés par l'ANSSI ;
- de se limiter à une seule version du produit et des fournitures : le commanditaire ou développeur ne peut mettre à jour ni le produit, ni les fournitures, pendant l'évaluation (sauf accord explicite du centre de certification de modification des fournitures).

Le déroulement de l'évaluation repose sur :

- la documentation fournie ;
- au minimum, les bases publiques de vulnérabilités pour l'analyse du produit par rapport aux vulnérabilités connues pour le type de produit analysé ;
- le produit lui-même, installé sur une plateforme de test aussi représentative que possible de son environnement prévu d'utilisation ;
- les éléments fournis pour réaliser l'analyse de la cryptographie (voir [CRY-P-01]).

[2] Ces méthodologies sont publiées sur la page du site de l'ANSSI consacrée aux critères et méthodologies d''évaluation CSPN (www.ssi.gouv.fr).

Les résultats sont consignés dans un RTE qui est transmis au centre de certification. Après sa validation par le centre de certification, le centre d'évaluation l'envoie également au commanditaire d'évaluation.

9.3 Contraintes imposées

L'évaluation est réalisée en temps et charge contraints afin de répondre à des exigences de maîtrise des coûts et des délais.

La charge de référence d'une évaluation CSPN est de 25 hommes.jours, dans un délai calendaire de 8 semaines. De plus, lorsque des fonctions de sécurité essentielles du produit reposent sur des mécanismes cryptographiques, la charge est augmentée de 10 hommes.jours.

La charge peut également être adaptée à la hausse, comme à la baisse, dans les cas suivants :

- sur demande du Centre de certification, en particulier lorsqu'une méthodologie particulière spécifiant une charge adaptée est appliquée ;
- sur proposition du CESTI[4].

Toutefois, cette charge ne doit pas être inférieure à 15 hommes.jours ni être supérieure à 60 hommes.jours.

9.4 Analyse de la conformité

L'analyse de la conformité se fait sur une plate-forme de test, qui doit être décrite dans le RTE.

L'objectif de cette phase est double. Il s'agit :

- d'une part, de vérifier que le produit est conforme à ses spécifications de sécurité, toutes les non-conformités découvertes devant être tracées et rappelées dans le RTE ;
- d'autre part, de permettre à l'évaluateur de bien comprendre le produit dans sa globalité pour être pertinent dans les analyses d'efficacité.

L'analyse de la conformité peut également comporter, lorsque cela est possible et que cela a du sens :

- une analyse des performances du produit ;
- une description éventuelle de l'interopérabilité du produit avec d'autres produits.

9.5 Analyse de l'efficacité

Les principaux objectifs de l'analyse de l'efficacité sont :

- de coter la résistance théorique des fonctions et des mécanismes de sécurité et, le cas échéant, des mécanismes cryptographiques ;
- d'identifier les vulnérabilités ;
- de donner un avis sur les risques de mauvaise utilisation ;
- de donner un avis d'expert sur l'efficacité du produit ;
- éventuellement, de proposer un paramétrage et un environnement d'utilisation qui permettent de limiter l'exploitabilité des vulnérabilités et, dans ce cas, de donner un second avis d'expert sur l'efficacité du produit dans son nouvel environnement d'utilisation.

[4] une justification sera nécessaire. Ci-après une liste non exhaustive de points pouvant justifier une adaptation de charge :

- TOE requérant un effort d'installation important risquant d'empiéter sur les charges d'évaluation ;
- grand nombre de fonctions de sécurité à évaluer ;
- présence de protocoles propriétaires ;
- réévaluation du même produit ;
- accès au code source ;
- etc.

9.6 Analyse d'impact sur la sécurité du système hôte

L'évaluation vérifiera en particulier que le produit ne dégrade pas la sécurité du système hôte[5]. C'est en particulier le cas lorsque le produit nécessite des privilèges particuliers sur le système hôte pour fonctionner.

9.7 Rapport technique d'évaluation

Le plan du RTE est imposé (voir [METHODE]).

10 Délivrance du certificat

10.1 Cas nominal

A l'issue de l'évaluation, le RTE est transmis au centre de certification de l'ANSSI. Le processus nominal de certification comporte les étapes suivantes :

1. Analyse et validation du RTE. L'ANSSI peut être amenée à demander des précisions, voire des travaux supplémentaires au centre d'évaluation si ceux-ci ne sont pas estimés suffisants.

   Le RTE peut indiquer le besoin de modifier des fournitures. Après analyse par le centre de certification de ces modifications, le centre d'évaluation peut transmettre ce besoin au commanditaire pour qu'il soit pris en compte.

   Le RTE ne sera validé qu'après réception des fournitures modifiées et de leur validation par l'évaluateur et le centre de certification.
2. Présentation des travaux et des résultats de l'évaluation par le centre d'évaluation à l'ANSSI[2]. A cette occasion, l'ANSSI peut demander que lui soit faite une démonstration du produit.
3. Rédaction du rapport de certification. Celui-ci précise notamment le périmètre et les fonctionnalités de sécurité objets de la certification. Il peut comporter tout avertissement que l'ANSSI estime utile de mentionner pour des raisons de sécurité. Il signale également les problèmes potentiels relevés lors de l'évaluation et qui sont susceptibles d'intéresser un utilisateur. Par défaut, il est rédigé en français, mais peut également être rédigé en anglais sur demande du commanditaire et si le CESTI l'accepte.
   Le projet de rapport de certification peut être communiqué au commanditaire et au CESTI avant validation.
4. Ce rapport est validé par le chef de centre ou son adjoint avant sa transmission pour signature. Le directeur général de l'Agence nationale de la sécurité des systèmes d'information, par délégation du Premier ministre, signe le rapport de certification. L'utilisation de la marque « Ti SECURITE CERTIFICATION » doit se faire conformément à la procédure [MAR-P-01].

10.2 Cas particulier

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 processus de certification est arrêté à l'issue de l'étape 1 ou 2.

Le commanditaire est averti de cette situation. Parmi les raisons pour lesquelles l'ANSSI peut estimer que le produit répond imparfaitement à sa cible de sécurité, on peut citer :

- une résistance trop faible des fonctions et des mécanismes de sécurité, et le cas échéant, des mécanismes cryptographiques ;
- le dysfonctionnement de certaines fonctions de sécurité ;
- le dysfonctionnement de certaines fonctionnalités du produit, n'en permettant pas un usage normal ;

[5] La définition de système hôte varie en fonction du type de TOE considéré : si la TOE est une application, le système hôte est le système d'exploitation. Si la TOE est un pare-feu, le système hôte est le SI sur lequel la TOE est déployée.

[2]Une fois le rapport d'évaluation validé par l'ANSSI, le commanditaire peut demander au CESTI une présentation de ce type

- l'impossibilité d'obtenir certaines informations nécessaires à la compréhension des fonctions de sécurité du produit, ne permettant pas d'estimer correctement la résistance des fonctions et des mécanismes de sécurité et des mécanismes cryptographiques le cas échéant ;
- l'impossibilité de disposer d'éléments suffisamment probants pour conclure à l'absence d'impact négatif du produit sur le système hôte.

11 Durée de validité

La certification d'un produit est délivrée pour une durée de validité de trois ans.

A l'issue de la période de validité, le certificat est retiré et archivé.

Si le certificat n'est pas public, sa validité peut être demandée par messagerie électronique au commanditaire de l'évaluation en mettant en copie le centre de certification. Ce dernier pourra alors confirmer ou infirmer la réponse qui sera fournie.

12 Continuité de l'assurance

Un certificat ne porte que sur une version précise d'un produit. En cas d'évolution de ce produit, les nouvelles versions ne sont pas certifiées par défaut. Le processus de continuité de l'assurance (voir [CONTINUITE]) permet de déterminer, à moindre coût, si une nouvelle version d'un produit peut bénéficier du certificat d'une version précédemment certifiée. Ce processus est applicable à la CSPN.

13 Publicité

13.1 Règles de communication

Le commanditaire peut faire état du fait de la certification CSPN du produit. Il doit le faire dans des termes honnêtes et compréhensibles pour l'utilisateur final. Il doit impérativement indiquer :

- la référence du certificat ;
- la date de certification du produit ;
- les références et la version du produit certifié ;
- la date de fin de validité du certificat .

Il doit également :

- délivrer des copies conformes aux originaux des rapports de certification et des cibles de sécurité si un donneur d'ordre en fait la demande ;
- ne pas faire d'annonce trompeuse sur le produit.

Il peut également mentionner l'adresse du site de l'ANSSI, sur lequel l'utilisateur peut consulter la cible de sécurité du produit et le rapport de certification.

L'ANSSI se réserve la possibilité de faire connaître, par tout moyen qu'elle considère nécessaire et efficace, tout usage abusif de la CSPN.

13.2 Règles d'utilisation de la marque

La marque « Ti SECURITE CERTIFICATION » peut être utilisée pour faire valoir l'obtention d'un certificat, sa description et ses modalités d'usage sont décrites par les procédures [MAR-P-01].

14 Suspension et retrait

14.1 Suspension de la certification

Le centre de certification de l'ANSSI peut être amené à suspendre la certification d'un produit si, par exemple :

- un fait nouveau lui permet de démontrer que des informations transmises par le commanditaire ou le développeur au cours de l'évaluation n'étaient pas exactes et qu'elles ont pu fausser le jugement des évaluateurs et donc le résultat final ;

- une vulnérabilité est découverte sur un produit certifié.

Le centre de certification informe sans délai le commanditaire et éventuellement communique les actions possibles qui permettraient de rétablir la certification.

Le commanditaire dispose alors d'un mois au maximum pour identifier les actions qu'il compte prendre pour rétablir la situation.

A l'issue de ce mois, plusieurs cas sont à envisager :

- si le centre de certification considère que les actions proposées ne répondent pas à la problématique ou si le commanditaire prend la décision de ne pas rétablir la situation, les documents publiés sont alors archivés ;
- si le centre de certification estime que le plan d'actions fourni par le commanditaire est adapté, le commanditaire dispose alors de trois mois au maximum pour mettre en œuvre son plan d'actions et fournir la preuve (par exemple en fournissant les résultats d'une réévaluation) au centre de certification que les actions entreprises, conformément au programme de certification, ont bien permis de résoudre définitivement la situation.

Deux cas sont alors possibles :

- soit après examen des preuves, le centre de certification estime les résultats adaptés, la suspension est levée ;
- soit les preuves ne répondent pas à la problématique, le certificat est alors retiré.

Le centre de certification dispose d'un mois pour statuer sur ces deux cas possibles.

14.2 Retrait de la certification

Le centre de certification est amené à retirer une certification si, par exemple :

- la date de validité de certification d'un produit est dépassée (voir chapitre 11) ;
- la période d'un mois, pour permettre au commanditaire de présenter les actions qu'il compte prendre suite à une suspension, est dépassée ;
- le plan d'actions, proposé par le commanditaire pour remédier à la suspension, est inadapté ;
- la période de trois mois pour la mise en œuvre du plan d'actions est dépassée.

Le centre de certification de l'ANSSI peut également retirer une certification si, par exemple :

- l'utilisation ou l'affichage du rapport de certification ou du certificat est effectuée de manière frauduleuse, erronée ou abusive ;
- l'utilisation ou l'affichage de la marque « Ti SECURITE CERTIFICATION » est frauduleuse, erronée ou abusive ;
- les engagements de certification ne sont pas respectés scrupuleusement.

Dès que le centre de certification a connaissance de l'un de ces motifs, il en informe par courrier électronique et sans délai le commanditaire et, éventuellement, communique les actions possibles qui permettraient de maintenir la certification. Le commanditaire dispose alors de quatre semaines au maximum pour rétablir la situation, sinon la certification est retirée.

L'ANSSI communique sur le retrait par tout moyen qu'elle juge approprié afin que les utilisateurs du produit certifié soient informés, notamment au travers du retrait des documents publiés sur le site de l'ANSSI.

14.3 Information du commanditaire

Une fois validée par le chef de centre ou son adjoint, la décision de suspension ou de retrait est adressée au commanditaire par courrier du directeur général de l'ANSSI dès lors que le motif de retrait n'est pas lié à la fin de période de validité du certificat ou à une décision du commanditaire. Dans ces deux derniers cas, les conditions de retrait étant décrites dans la présente procédure de certification, elles ne sont donc pas rappelées au commanditaire avant exécution du retrait.

Quel qu'en soit le motif, le commanditaire doit impérativement et immédiatement cesser d'utiliser l'ensemble des moyens de communication qui fait référence au certificat dès lors que celui-ci est suspendu ou retiré.

15 Réduction de portée d'un certificat

Seule une réévaluation permet de reconsidérer la portée d'un certificat précédemment émis.

16 Appel de la décision

Le commanditaire peut faire appel de toute décision du centre de certification afin que la décision soit reconsidérée (voir [ANO-P-01]).

ANNEXE A. Références

Référence	Document
[AGREMENT]	Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau, référence ANSSI-CSPN-AGR-P-01, version en vigueur.
[CRITERES]	Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référenceANSSI-CSPN-CER-P-02, version en vigueur.
[METHODE]	Méthodologie d'évaluation en vue d'une certification de sécurité de premier niveau - et Contenu et structure du RTE, référence ANSSI-CSPN -NOTE-01, version en vigueur.
[DOSSIER_EVAL]	Dossier de demande d'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-F-01, version en vigueur.
[CONTINUITE]	Maintien de la confiance, continuité de l'assurance, référence ANSSI-CSPN-MAI-P-01, version en vigueur.
[MAR-P-01]	Utilisation de la marque "Ti SECURITE CERTIFICATION", référence ANSSI-CC-MAR-P-01, version en vigueur.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P-01, version en vigueur.
[ANO-P-01]	Traitement des anomalies, référence ANSSI-CC-ANO-P-01, version en vigueur.
[NOTE-06]	Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, référence ANSSI-CSPN-NOTE-06, version en vigueur.
[GD-CSPN]	Liste des guides d'application obligatoire pour un produit visant une certification CSPN : - Recommandations relatives à l'authentification multifacteur et aux mots de passe, version en vigueur, disponible sur https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/ - Recommandations de sécurité relatives à TLS, version en vigueur, disponible sur https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/ - Recommandations de configuration d'un système GNU/Linux, version en vigueur, disponible sur https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/
[PP-CSPN]	Liste des profils de protection utilisables pour un produit visant une certification CSPN : - Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés), version en vigueur, disponible sur https://www.ssi.gouv.fr/guide/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies/

	- Profils de protection pour les systèmes industriels, version en vigueur, disponibles sur https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/

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

ANNEXE B. Eligibilité à la certification CSPN

a. Limitations liées à l'état de l'art

Le centre de certification refusera la certification pour les produits ou technologies au sujet desquels il ne dispose pas d'un état de l'art. Entre autres conséquences, cela implique que seules les fonctionnalités suivantes peuvent être utilisées comme fonctions de sécurité dans des cibles de sécurité :

- Communication sécurisée ;
- Identification, authentification et contrôle d'accès des utilisateurs[6] ;
- Protection de données, en stockage ou en transit, incluant l'effacement sécurisé ;
- Fonctions cryptographiques et générateurs de nombres aléatoires ;
- Autoprotection : démarrage sécurisé, autotests, protection physique, cloisonnement… ;
- Journalisation.

Les autres fonctionnalités de sécurité d'un produit, en particulier les fonctions d'analyse ou de détection (pare-feu applicatif, filtrage de fichiers, fonctions de détection d'intrusion, scan de vulnérabilités…), ne pourront donc pas être évaluées[7]. Elles ne seront considérées que sous l'angle de la surface d'attaque qu'elles induisent sur le produit.

b. Limitations liées aux règles et à l'esprit de la CSPN

Le centre de certification refusera la certification à toute TOE dont la cible de sécurité est considérée comme **incompatible avec les règles ou l'esprit de la CSPN**. Ce refus pouvant intervenir à l'enregistrement comme en fin d'évaluation, les commanditaires sont invités à s'assurer que leurs cibles de sécurité sont bien éligibles. Des exemples sont fournis ci-après :

Cas typiques	Exemples	Comment rendre le produit éligible ?
Produit présentant un trop grand nombre de fonctions de sécurité pour les charges d'une évaluation CSPN	Grand nombre de protocoles complexes ou propriétaires. Fonctions multiples, p.ex. de pare-feu *et* de VPN.	Effectuer plusieurs évaluations en séquence : d'abord en désactivant une partie des fonctions[8], puis dans une configuration complète.
Produit présentant un trop grand nombre de composants pour les charges d'une évaluation CSPN	Serveur avec nombreux types de clients (iOS, Android, Windows, Linux, etc.)	Effectuer plusieurs évaluations en séquence : d'abord avec un seul client représentatif, puis en ajoutant les autres clients.

[6] La CSPN permet d'évaluer des mécanismes d'authentification se basant sur des mots ou phrases de passe, ainsi que de la cryptographie symétrique ou asymétrique standard. Elle ne permet pas d'évaluer les mécanismes d'authentification biométriques ni les systèmes d'enrôlement (par exemple les systèmes de type *Know Your Customer*).

[7] Il est possible pour le commanditaire de financer le centre d'évaluation pour proposer la définition d'une méthode d'évaluation pour de nouvelles technologies ou de nouvelles fonctionnalités de sécurités, et de la faire valider par le centre de certification. Cette validation s'appuiera notamment sur des travaux d'expertise de type CSPN (charge et activités comparables à une CSPN).

[8] Cette évaluation sera non publique si la configuration est non représentative de l'usage final, voir ANNEXE B.c

Cas typiques	Exemples	Comment rendre le produit éligible ?
Produit présentant un trop grand nombre de fonctions non évaluées, ou des fonctions non évaluées trop complexes, créant ainsi une surface d'attaque trop large ou impossible à analyser dans les charges de la CSPN	Produit mettant en œuvre des moteurs d'analyse ou de détection[9] Portail web massivement multiservice (messagerie, agenda, VoIP, travail collaboratif…)	Implémenter dans le produit des mécanismes de défense en profondeur d produit et les faire évaluer en ajoutant à la cible : - une menace considérant les fonctions non évaluées comme *compromises par défaut* ; - une fonction de sécurité d'autoprotection garantissant que cette compromission n'impacte pas les biens sensibles ou l'hôte de la TOE[10].
Produit « à la frontière du service », dont la configuration, l'installation ou l'administration est maîtrisée uniquement par le développeur et non l'utilisateur final	Produit ne pouvant être configuré, installé ou administré en pratique sans l'assistance du développeur. Produit présentant une interface non déclarée, utilisable par le développeur (par exemple distribution distante de mises à jour).	Permettre à l'utilisateur d'installer et utiliser le produit de façon autonome et. fournir, avec le produit, les guides correspondants. Déclarer dans la cible les fonctions de sécurité utilisées par le développeur afin que l'évaluateur vérifie leur robustesse. Pour les produits de type SaaS, se conformer à [NOTE-06]
Produit présentant des adhérences sur un service tiers	Portail web multiservice utilisant un service cloud tiers pour fournir par exemple la partie VoIP.	Permettre à l'utilisateur de désactiver les adhérences vers les services fournis par un tiers.
Produit dont l'évaluation se limiterait à une vérification de conformité	SDK, middlewares ou bibliothèques. Produit de chiffrement pour lequel le seul risque considéré est l'attaque des chiffrés produits.	Effectuer une évaluation de l'application utilisatrice du SDK plutôt que du SDK lui-même.
Produit au-dessous de l'état de l'art	Produit manifestement au-dessous de l'état de l'art « grand public »[11] ou n'adhérant pas aux guides obligatoires [GD-CSPN]	Mettre à jour la conception du produit pour le rendre à l'état de l'art.

[9] P.ex. sonde réseau, EDR, antivirus, pare-feu applicatif, scanner de vulnérabilités…

[10] Par exemple pour une sonde réseau, le développeur peut isoler les moteurs d'analyse dans des VM pour limiter l'impact de la compromission

[11] Produits de communication sécurisée sans protection de bout en bout, Produits de stockage sécurisé en ligne n'offrant pas de *perfect forward secrecy*….

Cas typiques	Exemples	Comment rendre le produit éligible ?
Produit incluant ou basé sur un composant tiers ne faisant pas l'objet d'un suivi de vulnérabilités[12].	Composant en version beta Composant dont le développeur a abandonné la maintenance Composant open source, maintenu par son développeur mais très peu diffusé en ne faisant pas l'objet d'un suivi réel par la communauté. Composant COTS dont le maintien en condition de sécurité est payant, et que le développeur n'aurait pas acheté	Mettre à jour les composants tiers afin de disposer du support du développeur originel de ces composants.
Produit utilisant des mécanismes cryptographiques entrainant une charge d'évaluation très importante, du fait de leur originalité.	Produit qui utilise des primitives cryptographiques propriétaires s'éloignant notablement de mécanismes cryptographiques standards.	Désactiver les primitives cryptographiques non standard.

c. TOE trompeuses ou non représentatives de l'utilisation réelle du produit

Le centre de certification refusera la certification à toute TOE trompeuse ou non représentative de l'utilisation réelle du produit Ce refus pouvant intervenir à l'enregistrement comme en fin d'évaluation, les commanditaires sont invités à s'assurer que leurs TOE sont bien éligibles. Des exemples sont fournis ci-après pour les y aider.

Cas typiques	Exemples
TOE configurée ou évaluée dans des conditions ne reflétant pas son usage réel, ou dont l'usage réel est impossible à déterminer.	Automate bancaire destiné à un accès public, mais dont la cible de sécurité ne considère pas les menaces physiques. Automate industriel sur lequel tous les protocoles industriels sont désactivés. Produit de signature électronique sur lequel la présentation de données à signer est désactivée.
TOE dont le problème de sécurité est mensonger, ou vide, ou	Cible présentant des hypothèses fausses ou notoirement non réalistes[13].

[12] Les composants tiers non supportés augmentent la surface d'attaque : l'absence de support entraîne l'impossibilité de se baser sur l'analyse de CVE pour juger de l'absence de vulnérabilités, ce qui rend la CSPN non pertinente. De plus, l'absence de support de ces composants rendra impossible ou incomplet le suivi des vulnérabilités post-certification.

[13] C'est-à-dire lorsque le produit fait une hypothèse de sécurité sur un service tiers pourtant notoirement reconnu comme non fiable (p.ex. utilisation du SMS comme second facteur d'authentification, utilisation de protocoles tiers vulnérables comme NTLMv1, etc.)

Cas typiques	Exemples
ne correspondant pas au type de produit auquel elle appartient.	Produit déployé dans un local sécurisé sans accès réseau, et dont tous les utilisateurs sont considérés de confiance. Produit décrit comme « stockage réseau sécurisé », dont la cible considère le contrôle d'accès réseau mais pas le stockage sécurisé. Pare-feu dont la cible ne considère comme fonction de sécurité que l'authentification de l'utilisateur permettant la modification de la configuration.
Composants isolés d'un produit complet	Bibliothèques, modules.