PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 12 avril 2021

N° **958/ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CSPN-CER-P-01_v3.0**

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.

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.

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 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 des commanditaires, 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.

Il peut demander à être destinataire du rapport technique d'évaluation (RTE) ou d'une version allégée de ce rapport.

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 dans lequel le produit fonctionne (modèle d'ordinateur, système d'exploitation, etc.),
    - les biens sensibles que le produit doit protéger,
    - les menaces contre lesquelles le produit offre une protection,
    - les fonctions de sécurité implémentées par le produit pour parer les menaces identifiées. Ce sont ces fonctions qui feront l'objet de l'évaluation[1] ;
- qu'il dispose d'une documentation permettant à un utilisateur final d'utiliser le produit de façon sûre (documentation utilisateur, éventuellement d'administration et d'installation) ;
- si des fonctions de sécurité essentielles du produit reposent sur des mécanismes cryptographiques, qu'il dispose de la documentation décrivant ces mécanismes, ainsi que de jeux de tests permettant à l'évaluateur de vérifier la conformité des mécanismes implémentés à leur description, conformément à [CRY_P_01] ;
- que le produit peut être associé à un ou plusieurs des domaines techniques d'agrément CSPN (cf. [AGREMENT]) ;

  Nota : si le produit n'entre dans aucune de ces catégories ou en cas de doute, le commanditaire peut contacter le centre de certification afin de déterminer si le produit est évaluable au sens de la CSPN, et si c'est le cas, le ou les centres d'évaluation qui pourraient réaliser l'évaluation ;
- que si une méthodologie d'évaluation CSPN spécifique existe pour ce type de produit, c'est bien cette méthodologie qui est retenue et que le produit répond aux exigences éventuelles contenues dans cette méthodologie ;
- que le centre d'évaluation pourra disposer d'un accès au produit ;
- que le centre d'évaluation pourra disposer d'un accès à des équipements de test si ceux-ci sont spécifiques ou dédiés ;

[1] Dans le cas où le produit nécessite des privilèges particuliers pour s'exécuter sur le poste de l'utilisateur, l'évaluation portera davantage sur la non-altération de la sécurité du système hôte que sur les fonctionnalités propres au produit.

- 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 :

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

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 :

- demande incomplète ;
- cible de sécurité incomplète ;
- cible de sécurité manifestement trompeuse (par exemple, le produit est un pare-feu et la seule fonction de sécurité décrite comme devant être évaluée est l'authentification de l'utilisateur pour modifier la configuration de son produit) ;
- centre d'évaluation non agréé pour le domaine technique du produit ;
- produit dont la complexité est telle qu'il n'est pas envisageable de réaliser une évaluation dans le cadre de la CSPN ;
- refus du commanditaire d'informer le centre de certification sur les vulnérabilités potentielles du produit ;
- non-respect des prérequis identifiés au chapitre 5.

9 Déroulement de l'évaluation

9.1 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.

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

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

- la conformité du produit à sa cible de sécurité (§ 9.3) ;
- l'efficacité des fonctions de sécurité (§ 9.4) ;
- 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 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]).

Les résultats sont consignés dans un RTE qui est transmis au centre de certification.

9.2 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 :

- lorsqu'une méthodologie particulière spécifiant une charge adaptée est appliquée ;
- sur proposition du CESTI ;
- sur demande du Centre de certification.

Toutefois, cette charge ne doit pas être inférieure à 15 hommes.jours ni être supérieure à 50 hommes.jours. En cas de demande de modification par le CESTI, une justification sera nécessaire. Ci-après une liste non exhaustive de points pouvant justifier une adaptation de charge :

- grand nombre de fonctions de sécurité à évaluer ;
- présence de protocoles propriétaires ;
- réévaluation du même produit ;
- accès au code source ;
- etc.

9.3 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.

9.4 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.

9.5 Analyse d'impact sur la sécurité du système hôte

Dans le cas où le produit nécessite des privilèges particuliers sur le système hôte pour fonctionner, l'évaluation vérifiera en particulier que le produit ne dégrade pas la sécurité du système hôte.

9.6 Rapport technique d'évaluation

Le RTE comporte au minimum les informations suivantes :

- un rappel du contexte de l'analyse (contexte d'emploi, durée de l'analyse et fonctions de sécurité notamment) ;
- une synthèse de la documentation donnant une description des fonctions de sécurité ou liées à la sécurité ;
- ce qui est attendu fonctionnellement du produit (résumé de ses caractéristiques de sécurité notamment) ;
- un inventaire des vulnérabilités du produit (informations issues du CERT-FR, de bases publiques ou du développeur) et des correctifs disponibles applicables ;
- une liste des principaux outils d'analyse utilisés ;
- une synthèse des résultats des tests effectués sur le produit ;
- une cotation de la résistance des mécanismes de sécurité et des mécanismes cryptographiques le cas échéant ;
- un bilan et une cotation des éventuelles vulnérabilités exploitables identifiées ;
- un avis sur l'ergonomie du produit et des préconisations d'utilisation ou de paramétrage dans le contexte d'emploi prévu.

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

10 Certification

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 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.
2. Présentation des travaux et des résultats de l'évaluation par le centre d'évaluation. A cette occasion, l'ANSSI peut demander que lui soit faite une démonstration du produit. Le commanditaire de l'évaluation peut être invité à cette présentation.
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. Il est rédigé en français.

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 projet de rapport de certification. L'utilisation de la marque « Certification Sécurité TI » 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 ;
- 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 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.

12 Publicité

12.1 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.

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.

12.2 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].

13 Suspension et retrait

13.1 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.

13.2 Retrait de la certification

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

- 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.

13.3 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 une décision du commanditaire.

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.

14 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-CER-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 sécurité 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.

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