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 26 novembre 2020

N° **2672 /ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CC-SUR-P-01_v5.0**

PROCEDURE

SURVEILLANCE DES PRODUITS CERTIFIES

Application **:** A compter de novembre 2020.

Diffusion **:** Publique.

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

Renaud LABELLE
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

SUIVI DES MODIFICATIONS

Version	Date	Modifications
1	28/10/2003	Création
2	30/08/2005	Modification des conditions d'arrêt de la surveillance et de la périodicité
3	19/12/2013	Changement de dénomination de l'organisme de certification (ANSSI) et améliorations de forme Mise à jour des références Prise en compte des produits maintenus dans le cadre du processus de surveillance Ajout du cas de l'évolution des guides Ajout du cas de l'évolution des sites de développement ayant fait l'objet d'un audit Ajout de l'émission d'un rapport de surveillance par l'ANSSI Intégration de l'instruction « SUR/I/01.1 Surveillance pour le GIE-CB » qui devient obsolète dès l'approbation de cette procédure
4.0	19/06/2017	Ajout des formulaires concernés par cette procédure Prise en compte du formulaire de satisfaction client
4.1	08/01/2020	Pour être conforme aux pratiques actuelles, la publication des résultats sur le site de l'ANSSI et ceux des accords de reconnaissance est supprimée.
5.0	26/11/2020	Précision apportée sur les avis soumis au comité directeur de la certification Ajout d'un paragraphe précisant les conditions d'enregistrement et de conservation des documents Mise en conformité avec les nouvelles directives du SOG-IS concernant la validité des certificats Prise en compte 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

Cette procédure décrit le processus de surveillance des produits. La surveillance a pour objectif d'assurer dans la durée, la confiance dans les produits certifiés et maintenus, ou plus précisément la confiance en leur résistance aux attaques, en tenant compte de l'évolution de l'état de l'art dans le domaine des attaques.

La surveillance s'inscrit dans le cadre du décret 2002-535 et suit les procédures du système de certification.

2 Description de la procédure

La surveillance consiste à réaliser de manière périodique des travaux de mise à jour de l'analyse de la résistance du produit certifié et de ses éventuelles maintenances.

2.1 Portée de la surveillance

La surveillance porte sur les produits certifiés [CER-P-01] ou qui ont été maintenus dans le cadre de la procédure de maintenance [MAI-P-01]. Les dernières versions des guides référencées dans les rapports sont prises en compte.

2.2 Demande de mise sous surveillance

La surveillance d'un produit certifié et de ses éventuelles maintenances peut être demandée par le commanditaire de l'évaluation, le développeur du produit ou par toute autre personne ayant le consentement du développeur. Par mesure de simplification, seul le terme de « commanditaire » sera utilisé dans la suite du document.

Le processus de surveillance peut être initié à tout moment, soit juste après l'évaluation, soit plus tard.

Seul un centre d'évaluation ayant une parfaite connaissance du domaine pourra être sélectionné pour mener à bien la surveillance (typiquement, le centre d'évaluation ayant réalisé l'évaluation initiale du produit). Pour l'enregistrement de la surveillance par l'ANSSI, le commanditaire doit renseigner le formulaire de demande de surveillance [SUR-F-01] en y indiquant notamment la périodicité prévue de ces travaux.

La signature de ce formulaire signifie l'engagement du commanditaire à financer les travaux de surveillance (art. 3 du [DECRET]) et à prendre en charge les éventuelles livraisons des échantillons des produits au centre d'évaluation et au centre de certification.

La contre-signature de ce formulaire par le centre d'évaluation signifie qu'il s'engage à assurer une veille technologique sur l'état de l'art dans le domaine technique associé au produit certifié.

2.3 Travaux de surveillance

Pour les certificats non archivés, des travaux de surveillance peuvent être demandés à tout moment par le centre de certification (sur sa propre initiative ou sur la proposition d'un centre d'évaluation) afin que l'analyse de la résistance du produit sous surveillance fasse l'objet d'une mise à jour dans le cadre de la présente procédure suite, par exemple, à l'évolution de l'état de l'art.

Il convient de souligner que :

- seules les tâches relatives à la famille AVA_VAN doivent être rouvertes traduisant ainsi l'interdiction, pour le commanditaire, de modifier le produit certifié initialement ;
- la validité des résultats de la classe ALC doit être confirmée par le centre d'évaluation. Cette disposition conditionne l'apposition du logo SOG-IS sur le certificat.

L'analyse de la résistance du produit comprend :

- une analyse des mécanismes cryptographiques (uniquement si elle avait été initialement effectuée) intégrée à l'analyse de vulnérabilité mentionnée ci-dessous ;
- une analyse de vulnérabilité (en général, au même niveau que celle demandée dans la cible de sécurité du produit certifié) amenant éventuellement à la réalisation de tests de pénétration sur le produit avec de nouvelles méthodes. A cette occasion, de nouveaux tests de pénétration peuvent également être effectués pour évaluer les vulnérabilités initialement considérées comme résiduelles ou pour étudier des vulnérabilités qui n'auraient pas été prises en compte lors de l'évaluation initiale.

A l'issue de son analyse, le centre d'évaluation émet un rapport technique de surveillance qui est transmis au centre de certification et au commanditaire. Ce rapport établit le niveau de résistance

mis à jour. Le centre d'évaluation met également à jour[1] l'*ETR for Composite Evaluation*, tel que défini dans [COMP], lorsqu'il existe.

Dans la suite de cette procédure, le rapport de surveillance et les résultats qu'il contient sont définis comme étant positifs, si le niveau AVA_VAN de la certification initiale est confirmé. Sinon, les résultats et le rapport sont dits négatifs.

Evolution des guides :

L'ajout de recommandations de sécurité dans les guides des produits est autorisé dans le cadre de la présente procédure de surveillance. Le commanditaire doit alors fournir les nouveaux guides du produit et la nouvelle cible de sécurité si celle-ci, dans sa version initiale, référencie les guides.

Le centre d'évaluation doit alors établir le niveau de résistance des produits dans le cas de la mise en œuvre des nouveaux guides, ainsi que dans le cas de l'application des guides antérieurs.

Evolution des sites audités

La procédure de maintenance [MAI-P-01] permet la prise en compte d'une mise à jour de la liste des sites audités dans le cadre de l'analyse du cycle de vie du produit. Si le centre de certification ou le centre d'évaluation le juge nécessaire, le commanditaire doit fournir des échantillons produits selon le nouveau cycle de vie pour mener à bien les travaux de surveillance.

A noter que :

- les produits dont les certificats sont archivés depuis plusieurs mois ne pourront plus faire l'objet d'une nouvelle surveillance ;
- une tolérance est admise par le centre de certification dans le cas où le commanditaire « retardataire » n'aurait pas répondu dans les délais pour faire connaître sa position de publication ou non et dont le certificat aurait été archivé par défaut.

2.4 Décision de surveillance

Après validation du rapport technique de surveillance (et de l'*ETR for Composite Evaluation*, le cas échéant), la décision de surveillance est prise par le centre de certification via l'édition d'un rapport de surveillance, identifiant le(s) niveau(x) de résistance des produits.

Le rapport est ensuite transmis au directeur général de l'ANSSI qui le signe.

Un exemplaire du rapport signé est envoyé au commanditaire mentionné dans la demande de surveillance accompagné du formulaire de satisfaction client [QUA-F-03].

2.5 Publication

Une fois les résultats de la surveillance connus, le commanditaire dispose d'un mois pour faire part de sa décision de publication en adressant un courrier électronique au certificateur en charge de la surveillance.

Sans retour du commanditaire, la décision par défaut retenue par le centre de certification sera celle de ne pas publier les résultats.

Les conditions de publication sont décrites dans l'annexe B. Si la publication d'un rapport de surveillance positif est autorisée par le commanditaire (voir annexe B), le centre de certification édite un nouveau certificat sur lequel figure le même niveau AVA_VAN que celui mentionné sur le

[1] Nouvelle version ou addendum séparé

certificat précédent et comporte la nouvelle date de validité. Ce certificat est ensuite signé par le directeur général de l'ANSSI tandis que le rapport de surveillance est publié sur le site de l'ANSSI.

Concernant le cas d'un certificat initial non public et surveillé, il est de la responsabilité du gestionnaire de risques du produit de déterminer la validité de la certification sur la base des résultats de la surveillance, le centre de certification ne se prononçant pas sur l'extension de la validité.

Quel que soit le résultat obtenu, il appartient au commanditaire de signaler à ses clients le résultat de la surveillance (sauf dans les cas décrits en Annexe D).

2.6 Arrêt de la surveillance

La surveillance s'arrête :

- soit à la demande du commanditaire par courriel adressé à certification@ssi.gouv.fr et au certificateur (voir annexe C) ;
- soit par décision de l'ANSSI, en particulier, lorsque le rapport technique de surveillance n'est pas fourni à la date prévue au centre de certification.

ANNEXE A. Références

Référence	Document
[DECRET]	Décret 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.
[17065]	Norme EN ISO/IEC 17065 : Exigences pour les organismes certifiant les produits, les procédés et les services, version en vigueur.
[COMP]	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[CER_VALID]	*SOG-IS Recognition Agreement Management Committee - Certificate validity*, version 1.0.
[ASS_CONT]	*Joint Interpretation Library - Assurance continuity*, version 1.0, Novembre 2019.
[CER-P-01]	Procédure de certification critères communs de la sécurité offerte par les produits, les systèmes de technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version en vigueur.
[MAI-P-01]	Continuité de l'assurance, référence ANSSI-CC-MAI-P-01, version ne vigueur.
[SUR-F-01]	Demande de surveillance, référence ANSSI-CC-SUR-F-01, version ne vigueur.
[QUA-F-03]	Enquête de satisfaction client, référence ANSSI-CC-QUA-F-03, version ne vigueur.

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

ANNEXE B. Extension de la validité des certificats de produit

Résultat de la surveillance	Conditions minimales à satisfaire	Publication du rapport de surveillance	Non publication du rapport de surveillance
Positif : le niveau VAN du certificat initial est confirmé	1. Le périmètre fonctionnel de la surveillance doit être identique à celui de l'évaluation de la TOE initiale. 2. Les taches ALC doivent être confirmées pour disposer de la reconnaissance SOG-IS. 3. Les vulnérabilités identifiées par le centre d'évaluation devront être déclarées à CERT_FR. 4. Le cas échéant, les vulnérabilités doivent avoir été totalement résolues par l'ajout de recommandations dans les guides.	La date de validité du certificat initial est modifiée pour correspondre à la date du rapport de surveillance plus cinq ans. Puis, pour chaque nouvelle surveillance, la date de validité est modifiée pour correspondre à la date du dernier rapport de surveillance augmentée de cinq ans.	La date de fin de validité demeure inchangée, elle reste celle fixée lors de la certification initiale.
Négatif : le niveau VAN du certificat initial n'est pas confirmé	1. Le périmètre fonctionnel de la surveillance doit être identique à celui de l'évaluation de la TOE initiale. 2. Les taches ALC doivent être confirmées pour disposer de la reconnaissance SOG-IS. 3. Les vulnérabilités identifiées par le centre d'évaluation devront être déclarées à CERT_FR.	La date de validité du certificat initial reste inchangée.	Le certificat initial est considéré comme n'étant plus valide, les documents publiés sont alors archivés.

Pour plus de précision, se reporter aux documents [CER_VALID] et [ASS_CONT].

ANNEXE C. Modèle de courrier pour l'arrêt de la surveillance par le commanditaire

A adresser à : certification@ssi.gouv.fr
certificateur du produit

Objet : arrêt de la surveillance d'un produit certifié

Référence : 1) certificat <n° de certificat du produit>

Conformément à la procédure ANSSI-CC-SUR-P-01 du schéma français d'évaluation et de certification, je vous informe que je mets fin au processus de surveillance du produit cité en référence 1.

A <lieu>, le <date>

[Nom, titre, signature de la personne habilitée à engager la société,

ou mandataire social de la société]

ANNEXE D. Processus spécifiques de surveillance

Pour les produits sous surveillance au titre d'autres labels de l'ANSSI tels que la qualification ou de l'agrément des cartes bancaires par le GIE-CB, il est convenu avec ces donneurs d'ordre que :

- l'ANSSI les avertit de tout arrêt de la surveillance les concernant lorsqu'ils n'en sont pas à l'origine ;
- à leur demande, l'ANSSI leur fournit un état des produits sous surveillance les concernant.