Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 16 novembre 2005.

N° 3172/SGDN/DCSSI/SDR
Référence : SUR/P/01.2

PROCEDURE

SURVEILLANCE DES PRODUITS CERTIFIES

Objet : Surveillance des produits certifiés
Application : A compter du 1er décembre 2005
Diffusion : Publique

Vérifié par	Validé par Le sous-directeur de la "Régulation"	Vu l'avis du comité directeur sur la révision 1 Approuvé par Le Directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* [ORIGINAL SIGNE]	[ORIGINAL SIGNE]	[ORIGINAL SIGNE]

Suivi des modifications

Révision	Date	Modifications
1	28/10/2003	Création
2	30/08/2005	Modification des conditions d'arrêt de la surveillance et de la périodicité

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 le temps la confiance dans les produits certifiés, 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. Références

- Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- Norme NF EN 45011 : Chapitre 13 : surveillance.

3. Description de la procédure

3.1. Demande de la mise sous surveillance

La surveillance d'un produit certifié peut être demandée par le commanditaire de l'évaluation, le développeur du produit ou encore par toute autre personne ayant le consentement du développeur. Elle peut être initiée à tout moment, soit juste après l'évaluation, soit plus tard.

Seul un centre d'évaluation ayant une parfaite connaissance du produit pourra être sélectionné pour mener la surveillance du produit (typiquement, le centre d'évaluation ayant réalisé l'évaluation initiale du produit).

Pour l'enregistrement de la surveillance, le centre d'évaluation doit fournir à la DCSSI un dossier de surveillance qui précise l'organisation du projet de surveillance en termes de périodicité des travaux et de charges prévues. La surveillance est enregistrée lorsque ce dossier est validé par la DCSSI.

3.2. Portée de la surveillance

Un programme de surveillance ne porte que sur la version certifiée du produit.

3.3. Travaux de surveillance

La surveillance consiste à réaliser de manière périodique des travaux de mise à jour de l'analyse de résistance du produit certifié. Toutefois, le centre de certification peut à tout moment (sur sa propre initiative ou sur la proposition d'un centre d'évaluation) demander à ce que l'analyse de 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'apparition d'une nouvelle attaque).

Cette analyse de résistance comprend :

- une analyse de vulnérabilité (au même niveau que celui demandé dans la cible de sécurité du produit certifié) amenant éventuellement à des tests de pénétration sur le produit ;
- une analyse de la résistance des fonctions ;
- une analyse des mécanismes cryptographiques (uniquement si elle avait été initialement effectuée). Dans le cas où cette analyse laisserait apparaître une vulnérabilité, un rapport est transmis au centre d'évaluation afin qu'il essaie de l'exploiter et l'intègre comme point d'entrée à sa propre analyse de vulnérabilité.

A l'issue de l'analyse du centre d'évaluation, ce dernier émet un rapport qui est transmis au centre de certification et au commanditaire.

3.4. Arrêt de la surveillance

La surveillance peut être arrêtée :

- à la demande du commanditaire (voir modèle en Annexe A),
- par décision de la DCSSI, en particulier, en l'absence de rapport d'analyse à la date prévue.

4. Rôles des différents acteurs

4.1. Le commanditaire de la surveillance

Le commanditaire de la surveillance finance les travaux périodiques (art. 3 du décret 2002-535). Il est aussi en charge de la livraison des échantillons du produit au centre d'évaluation.

4.2. Le centre d'évaluation

Le centre d'évaluation en charge de la surveillance doit avoir une parfaite connaissance du produit (par exemple en ayant réalisé l'évaluation initiale du produit).

Il élabore le dossier de surveillance et assure une veille technologique sur l'état de l'art dans le domaine technique associé au produit certifié. A l'issue des travaux, il rédige le rapport contenant l'analyse de résistance du produit certifié et les résultats des tests (le cas échéant).

4.3. Le centre de certification

Le centre de certification suit l'ensemble des travaux de surveillance sur la base des résultats validés des travaux périodiques.

Il confirme la poursuite de la surveillance. Il est de la responsabilité du développeur de communiquer à ses clients les résultats de la surveillance.

Le centre de certification publie les résultats de la surveillance du produit uniquement sur demande du commanditaire de celle-ci.

Annexe A Modèle de lettre pour l'arrêt de la surveillance

A adresser à :

Monsieur le directeur central de la sécurité des systèmes d'information
SGDN/DCSSI
51, boulevard de la Tour-Maubourg
75700 Paris 07 SP

A l'attention du centre de certification (DCSSI/SDR/CCN)

Objet : arrêt de la surveillance d'un produit certifié
Référence : 1) certificat <n° de certificat du produit>

Monsieur le Directeur

Conformément à la procédure SUR/P/01 du schéma français d'évaluation et de certification, je vous informe que je met 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]