Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 13 juillet 2016

N° 2667/ANSSI/SDE/PSS/CCN

Référence :ANSSI-CC-NOTE-19/1.0

NOTE D'APPLICATION

MISE A JOUR DE LA TABLE DE COTATION DU DOCUMENT JIL " APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES "

Application : Dès son approbation

Diffusion : Publique

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

Guillaume POUPARD

[ORIGINAL SIGNE]

Suivi des modifications

Version	Date	Modifications
1.0	13/07/2016	Création

En application du décret n° 2002-535 du 18 avril 2002 modifié, la présente note d'application a été soumise au comité directeur de la certification, qui a donné un avis favorable.

La présente note d'application est disponible sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Table des matières

1. Présentation

1.1. Objet de la note

Cette note adapte la cotation de l'accès à la TOE réalisée lors d'évaluations Critères Communs (CC) du domaine « équipements matériels avec boîtiers sécurisés » au sein du schéma français, qui s'appuie sur le document [JIWG SB] émis en décembre 2015.

1.2. Référence

- [JIWG SB] : Joint Interpretation Library - Application of attack potential to hardware devices with security boxes, version 2.0, décembre 2015 (for trial use).

2. Cotation de la section « *access to TOE* »

Le document [JIWG SB] a été élaboré pour répondre aux besoins d'évaluation de type de produits « équipements matériels avec boîtiers sécurisés ». Il est destiné aux évaluations de produits de type routeurs, lecteurs sécurisés de cartes à puce, tachygraphes, HSM[1], etc.

Cependant, ce document ne s'applique correctement qu'aux équipements possédant des protections matérielles et logicielles notables. En effet, la section 2.2.5 *« Access to TOE »* du document accorde la cotation suivante :

Access to TOE (Samples)	Identification	Exploitation
Mechanical samples	1	1
Non functional samples	2	2
Fully functional samples	4	4

Où :

- *mechanical samples :* les échantillons sont non fonctionnels et peuvent être utilisés pour l'étude de la conception mécanique externe (mais pas à l'étude de la structure ou de la conception hardware interne) ;
- *non functional samples* : les échantillons sont non fonctionnels et peuvent être utilisés pour analyser la structure matérielle de la TOE, telles que des contre-mesures mises en place dans le produit ;
- *fully functional samples* : les échantillons sont entièrement fonctionnels avec leurs contre-mesures techniques externes désactivées ; l'*open sample* rentre aussi dans cette catégorie. Ils permettent d'effectuer de réelles simulations avec la TOE.

Avec la cotation actuelle, un produit disposant au final de protections matérielles faibles (ou facilement contournables), mais pour lequel l'attaquant doit avoir accès à un échantillon fonctionnel pour mener des attaques, peut réclamer directement 8 points dans la cotation de ces attaques, ce qui n'est pas justifié pour ces équipements.

[1] *Hardware Security Module.*

Pour prendre en compte de tels cas, la mise à jour suivante de la grille de cotation est à prendre en compte (en gras dans la table ci-dessous).

Access to TOE (Samples)		Identification	Exploitation
Mechanical samples	***with low hardware protection***	**Non applicable**	**Non applicable**
	with high hardware protection	1	1
Non functional samples	***with low hardware protection***	**1**	**1**
	with high hardware protection	2	2
Fully functional samples	***with low hardware protection***	**2**	**2**
	with high hardware protection	4	4

Où :

- *mechanical samples :* les échantillons sont non fonctionnels et peuvent être utilisés pour l'étude de la conception mécanique externe (mais pas à l'étude de la structure ou de la conception hardware interne) ;
- *non functional samples* : les échantillons sont non fonctionnels et peuvent être utilisés pour analyser la structure matérielle de la TOE, telles que des contre-mesures mises en place dans le produit ;
- *fully functional samples* : les échantillons sont fonctionnels et déverrouillés, c'est-à-dire fournis par le développeur dans un mode facilitant la mise en œuvre des attaques. Par exemple, les échantillons avec leurs contre-mesures techniques externes désactivées et l'*open sample* entrent dans cette catégorie ;
- *with low hardware protection* : protections matérielles faibles ou facilement contournables ;
- *with high hardware protection :* protections matérielles élevées et difficilement contournables.