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 7 juillet 2020
N° 1530/ANSSI/SDE/PSS/CCN

Référence :
ANSSI-CSPN-NOTE-07_v1.00

NOTE D'APPLICATION

METHODOLOGIE POUR L'EVALUATION DE SYSTEMES DE CONTROLE D'ACCES PHYSIQUE EN VUE D'UNE CSPN

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]

Suivi des modifications

Editions	Date	Modifications
0.1	21/06/2019	Document en état brouillon pour revue publique.
1.0	7/07/2020	Création du document définitif

TABLE DES MATIERES

1. Objet de la note

La présente note d'application précise les particularités de l'évaluation Certification de sécurité de premier niveau (CSPN) lorsqu'elle est appliquée aux systèmes de contrôle d'accès physique. La note affine les exigences de la méthodologie générique [P-CSPN-02].

1.1. Objectif

Cette note précise les éléments attendus de la part du commanditaire et du CESTI, lors d'une évaluation d'un système de contrôle d'accès physique. Elle vise également à clarifier l'état de l'art applicable, et peut donc imposer la prise en compte de certaines attaques, indépendamment des menaces définies dans la cible de sécurité.

1.2. Contexte et définitions

Les systèmes de contrôle d'accès physique visés par cette note sont constitués au moins des composants suivants[1]:

- un ou plusieurs lecteurs (ou têtes de lecture) ;
- une ou plusieurs Unités de traitement local (UTL[2]), qui assurent la gestion des lecteurs ;
- un centre de Gestion des accès contrôlés (GAC[3]), qui assure entre autres la journalisation des évènements et la gestion des données. Il inclut notamment les éléments suivants :
    - un logiciel de gestion du système, qui communique avec les UTL,
    - des ressources de type *base de données* ou *annuaire*, qui permettent de gérer les données essentielles au système, comme les droits, utilisateurs, groupes, ou encore identifiants de badges. Ces ressources peuvent appartenir à un système d'information extérieur au système évalué[4].

  Le GAC est composé principalement d'un ou plusieurs serveurs, d'équipements réseau ainsi que d'équipements de sécurité.

Le réseau dit *de gestion des accès* est constitué des interfaces entre ces différents composants du système, ainsi que :

- des dispositifs de verrouillage de portes ;
- des stations de gestion ou d'enrôlement ;

Le système peut s'interfacer avec :

- des badges[5] (ou supports similaires) ;
- tout ou partie d'un SI d'entreprise (ou partager des ressources avec ce SI, comme un annuaire ou une IGC) ;
- directement ou indirectement, des réseaux externes comme Internet.

---

[1] D'autres systèmes de contrôle d'accès ne présentent pas ce type d'architecture. Ils sont exclus du cadre d'application de cette note, et leur évaluation est soumise à une analyse au cas par cas.

[2] Également appelées unités de traitement et de contrôle.

[3] Également appelé centre de gestion des contrôles d'accès ou unité de traitement de supervision (UTS).

[4] Par exemple lorsque le système utilise directement un annuaire LDAP d'entreprise.

[5] Par souci de facilitation de la lecture, le terme « badge » sera utilisé de façon générique pour désigner tout type de support.

2. Organisation de l'évaluation

2.1. Eligibilité à la certification CSPN

Le centre de certification national (CCN) privilégie l'évaluation de systèmes complets mais autorise l'évaluation de composants isolés, dans le respect des règles suivantes :

- CCN pourra imposer de modifier le nom et le périmètre du produit soumis à évaluation afin que le produit certifié ne soit pas trompeur pour l'utilisateur final[6] ;
- la cible de sécurité décrira la configuration évaluée à l'aide du tableau ci-dessous :

Composant du système		**Inclus dans la cible de l'évaluation** (TOE)	**Non évalué** (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC	**Système d'exploitation**			
	Applicatifs			
	Fonctions cryptographiques			
	Bases de données et annuaires			
UTL	**Système d'exploitation**			
	Applicatifs			
	Fonctions cryptographiques			
	SAM			
Lecteurs	**Lecteurs simples**			
	Lecteurs-clavier			
Badges[7]				

Tableau 1 : Configuration d'évaluation du produit

Les cases de ce tableau seront renseignées avec les références et versions (logicielles et/ou matérielles) des composants concernés, y compris pour les composants fournis par des tiers (*Open source*, COTS…).

Chaque composant supposé « de confiance » fera l'objet d'une hypothèse dans la cible de sécurité. A l'inverse, chaque composant considéré comme « attaquant potentiel » sera considéré comme un attaquant dans la définition des menaces de la cible de sécurité.

[6] Par exemple, seuls les systèmes *complets* pourront être appelés « système de contrôle d'accès ».

[7] Cette note ne vise pas l'évaluation de badges. Seront listées ici les références des badges testés par l'évaluateur.

2.2. Charge d'évaluation

Les CESTI autorisés à mener les évaluations de systèmes de contrôle d'accès sont ceux agréés pour la portée « logiciel et équipement réseau ». Les charges et activités d'évaluation doivent respecter le tableau ci-dessous :

Activité d'évaluation	Charge nominale	Notes
Fonctions logicielles des UTL et lecteurs	**20 h*j**	Les activités d'évaluation doivent inclure l'analyse des échanges : - entre les UTL et les badges ; - au sein du système (entre GAC, UTL et lecteurs) ; - sur toute autre interface fonctionnelle.
Fonctions logicielles du GAC	**10 h*j**	Les activités d'évaluation doivent inclure l'analyse des échanges : - entre le logiciel de gestion du système et ses ressources (IGC, base de données ou annuaire, etc.), qu'elles fassent ou non partie de la TOE ; - avec l'extérieur du système : SI d'entreprise, Internet, etc. ; - sur toute autre interface fonctionnelle.
Sécurité matérielle	**5 h*j**	Les activités d'évaluation doivent inclure : - l'évaluation de la sécurité des interfaces matérielles de l'UTL et des lecteurs ; - l'analyse documentaire des badges.
Cryptographie	**5 h*j /** **10 h*j**	La charge est de **10 h*j** si les mécanismes cryptographiques sont implémentés par le produit lui-même, ou utilisent du code *open source*. S'ils sont implémentés par un composant en source fermée, alors la charge sera uniquement de **5 h*j**. L'évaluation se concentrera alors sur l'utilisation correcte des mécanismes sous-jacents. Le rapport de certification signalera que les mécanismes cryptographiques eux-mêmes ne sont pas évalués.

Tableau 2 : activités d'évaluation

La charge nominale est donc de 45 hommes*jours (si la cryptographie est implémentée par le produit), ou 40 hommes*jours (si la cryptographie est implémentée par un OS propriétaire).

Cette charge peut être revue à la hausse si le système est inhabituellement complexe (dans la limite de 50 hommes*jours). Elle peut également être réduite, par exemple si seul un composant isolé du système est soumis à évaluation.

2.3. Sous-traitance éventuelle des tests matériels

Concernant les tests matériels, le CESTI en charge de l'évaluation peut décider, selon ses compétences, de réaliser lui-même cette partie de l'évaluation[8], ou de la confier à un autre CESTI agréé sur ce domaine de compétence.

2.4. Fournitures

Il est de la responsabilité du CESTI de ne démarrer l'évaluation qu'une fois livré l'ensemble des fournitures nécessaires pour mener à bien l'évaluation. À titre de rappel, la [NOTE-20] autorise le CESTI à refuser une livraison incomplète ou de qualité insuffisante. Les fournitures requises par la CSPN sont *a minima* les fournitures listées ci-dessous.

1) fournitures matérielles :
   a) tous les composants de la TOE et de son environnement listés dans le tableau *Tableau 1 : Configuration d'évaluation du produit*. Les composants livrés au titre de la TOE doivent être fournis dans leur configuration dite *de production*[9] ;
   b) un moyen matériel ou logiciel permettant de simuler les dispositifs de verrouillage des portes, qui peut être une maquette physique.
2) fournitures logicielles :
   a) les éventuels moyens d'administration additionnels requis par la solution (si un logiciel dédié est nécessaire par exemple pour le provisionnement ou la mise à la clé, pour effectuer les mises à jour logicielles, etc.)
   b) le code source (non préprocessé) des mécanismes cryptographiques de la TOE;
   c) un micrologiciel permettant de tester la mise à jour logicielle des composants du système (si la mise à jour est incluse dans les fonctions de la cible de sécurité) ;
   d) les éventuelles licences requises par la solution.
3) fournitures documentaires :
   a) l'intégralité de la documentation d'installation, de configuration, d'administration et d'utilisation de l'ensemble du système, quel que soit le périmètre du produit évalué. Cela inclut notamment les guides relatifs aux procédures d'enrôlement des utilisateurs. Cela inclut également les composants du système fournis par des tiers (par exemple les lecteurs). ;
   b) la description des mécanismes cryptographiques.

[8] Cela nécessitera que le CESTI démontre sa capacité à le faire, dans le respect des règles d'agrément en vigueur.

[9] « Configuration de production » signifie ici que les composants sont dans un état « final », ou « dans l'état où ils seraient fournis à un client (ou un intégrateur) ». Cela s'oppose aux configurations de développement, de test, ou encore de maintenance, où les composants peuvent présenter des interfaces privilégiées (type JTAG) ou être configurés avec des mots de passe, clés ou certificats « de test ». Cela signifie aussi que toutes les contremesures (comme la détection d'arrachement) doivent être activées.

La configuration de production peut être une fourniture logicielle plutôt que matérielle, si cela correspond au format de livraison habituel du développeur (par exemple pour le logiciel de gestion du système).

3. Etat de l'art et consignes spécifiques pour l'évaluateur

Un système de contrôle d'accès doit prémunir l'utilisateur contre deux risques essentiels :

R1. entrée non autorisée dans les locaux ;
R2. dissimulation (non-détection par le système) d'une entrée dans les locaux.

L'évaluateur fondera principalement son avis sur la possibilité qu'a un attaquant de réaliser l'une ou l'autre de ces menaces essentielles[10].

3.1. Installation

L'évaluateur doit se prononcer sur les risques de mauvaise installation et l'exhaustivité des guides d'installation du développeur. Cela impose donc qu'il procède lui-même à l'installation logicielle[11] du produit. L'évaluateur pourra exiger des charges d'évaluation additionnelles si nécessaire.

À l'issue de l'installation, l'évaluateur s'assurera en particulier qu'une procédure permet de confirmer que les versions des composants installés correspondent à celles listées dans le *Tableau 1 : Configuration d'évaluation du produit.*

3.2. Analyse de la cible de sécurité

Le problème de sécurité défini dans la cible de sécurité doit *au minimum* répondre aux deux risques essentiels R1 et R2, sans quoi la cible sera considérée comme trompeuse.

Il est attendu que ces risques soient déclinés en listes de menaces, qui peuvent différer d'un système à un autre. Cette note n'impose pas de liste détaillée de menaces car une telle liste est amenée à évoluer en fonction des choix technologiques des développeurs et de l'état de l'art.

3.3. Analyse de vulnérabilités

3.3.1. Interprétation des vulnérabilités

Les vulnérabilités découvertes sur le produit devront être interprétées dans la perspective des risques essentiels du produit (R1 et R2)[12].

L'évaluateur doit notamment tenir compte du fait que les produits de contrôle d'accès physique visent à être déployés sur de longues durées (jusqu'à 10 ou 15 ans). L'évaluateur doit donc prendre en considération les risques de sous-dimensionnement de mécanismes cryptographiques, ou les risques liés à une longue durée d'exposition du produit (par exemple l'absence de mécanismes de mise à jour de *firmware* ou de clés).

---

[10] Étant entendu que chacune de ces menaces peut être réalisée par de nombreux moyens. Par exemple, l'*entrée non autorisée dans les locaux* peut découler d'une divulgation de secrets, de la modification non autorisée du firmware d'un composant, etc.

[11] L'installation matérielle peut être réalisée par l'évaluateur s'il dispose des compétences requises (notamment habilitation électrique). Cependant, on considèrera par défaut qu'elle est effectuée par le développeur.

[12] Exemples : une mauvaise protection des mises à jour logicielles sera un point d'attention, *même si cela n'est pas une fonction de sécurité explicite du produit*, car cela peut aider un attaquant dans la réalisation du risque R1. De la même manière, un processus d'enrôlement utilisateur non robuste pourra être considéré comme une vulnérabilité du produit, *même si la vulnérabilité provient de la documentation et non du logiciel ou du matériel.*

3.3.2. Surface d'attaque

Dans son argumentaire, l'évaluateur devra considérer les différents chemins d'attaque décrits dans le tableau ci-dessous.

Localisation de l'attaquant		**Attaques matérielles**	**Attaques logiques**
Sur site	Zone névralgique	L'attaque matérielle n'est pas considérée car la zone névralgique est supposée sûre.	Attaque via les **fonctions de gestion** du système (voir §A.2ii.) ou via la connexion au **réseau d'entreprise** (voir A.2iii)
	Zone protégée	Attaque matérielle des **UTL**[13] (voir §A.1i)	Attaque du **réseau de gestion des accès** (voir §A.2i) typiquement entre les UTL, ou entre UTL et logiciel de gestion du système.
	Zone publique	Attaque matérielle des **badges** ou **lecteurs** (voir §A.1ii)	Attaque du **réseau de gestion des accès** (voir §A.2i) typiquement entre lecteurs et UTL.
Hors site		Attaque matérielle de **tout composant** du système **avant installation** ou **après fin de vie** (voir §A.1iii)	Attaque via **Internet** (voir A.2iv)

Tableau 3 : Chemins d'attaque à considérer lors de l'évaluation

Chaque chemin d'attaque donne lieu à des points d'attention détaillés dans l'Annexe A. Ces points d'attention ne constituent pas pour autant une liste exhaustive de scénarios à étudier.

4. Références

[P-CSPN-02]	Procédure – Critères pour l'évaluation en vue d'une Certification de sécurité de premier niveau, Référence : ANSSI-CSPN-CER-P-02, version en vigueur.
[MET_CSPN]	Note d'application – Méthodologie pour l'évaluation en vue d'une Certification de sécurité de premier niveau – Contenu du RTE, Référence : ANSSI-CSPN-NOTE-01, version en vigueur.
[NOTE-20]	Note d'application – Règles relatives à la mise en œuvre des évaluations sécuritaires, Référence : ANSSI-CC-NOTE-20, version en vigueur.
[GUIDE-ACCES-PHYS]	Guide – Sécurité des technologies sans-contact pour le contrôle des accès physiques, version en vigueur

[13] La cotation doit donc prendre en compte l'effort requis pour accéder aux UTL, mais les attaques physiques ne sont pas exclues par principe.

Annexe A Points d'attention pour l'évaluateur

A.1 Attaques matérielles

L'évaluation de la sécurité des interfaces matérielles se limite à des attaques de difficulté relativement modérée[14] :

- identification des composants présents sur la carte électronique ;
- exploitation des interfaces de *debug* type JTAG ou UART ;
- extraction de mémoires flash (et reverse engineering éventuel) ;
- écoute des communications sur la carte électronique[15] ;
- détection d'arrachement et détection d'ouverture des boîtiers.

i. UTL

Si une SAM est présente, l'évaluateur doit prendre en compte les risques liés à son cycle de vie (provisionnement, renouvellements de clés, etc.), en particulier si elle est amovible et peut être manipulée hors de la zone protégée. L'évaluateur doit également vérifier que le système respecte les guides du développeur de la SAM afin d'éviter toute dégradation accidentelle de la sécurité. Enfin, comme pour tout composant tiers, l'évaluateur devra être attentif à la présence d'éléments non certifiés, et non maîtrisés par le développeur[16].

ii. Lecteurs et de l'interface avec les badges

L'évaluateur doit vérifier la robustesse du système contre les attaques exploitant l'interface sans-fil, en particulier l'attaque par relais[17].

iii. Tout composant avant installation ou après fin de vie

L'évaluateur doit vérifier si des biens sensibles peuvent être compromis avant installation ou après fin de vie des composants[18].

L'évaluateur prendra garde à considérer la compromission d'un bien sur un équipement mis au rebut, ou non encore installé, dans la perspective des risques essentiels R1 ou R2[19].

---

[14] Il n'est pas attendu que l'évaluateur fasse une preuve d'exploitation pour toutes les vulnérabilités matérielles identifiées. La détection d'ouverture, en particulier, sera cotée de façon purement théorique sur la base de l'expérience. Les preuves de concept seront à effectuer quand cela est nécessaire, par exemple pour démontrer la compromission par un port de *debug* ou la récupération de secrets en mémoire.

[15] Exemple : la récupération d'un PIN sur la nappe reliant le clavier au microcontrôleur d'un lecteur de badge.

[16] Exemple : une applet tierce non certifiée sur une SAM certifiée.

[17] Exemple : concernant l'attaque par relais, l'évaluateur peut vérifier que les badges et/ou les lecteurs implémentent des contremesures de type *distance bonding*, ou équivalentes.

[18] Exemple : l'évaluateur cherchera à démontrer la présence et l'efficacité de mécanismes du type :

- effacement des informations sensibles ;
- appairage ou autre mesure interdisant l'insertion d'un composant illégitime ou altéré ;
- protection des informations sensibles par contrôle d'accès, protection cryptographique logicielle ou utilisation d'un composant cryptographique matériel.

[19] Exemple : la compromission d'une clé diversifiée, sur un composant en fin de vie, ne sera pas nécessairement de nature à menacer le système. En revanche, l'attaquant pourrait exploiter la présence de clés non diversifiées sur des exemplaires disponibles à la vente.

A.2 Attaques logiques

i. Via le réseau de gestion des accès

Dans l'optique du risque essentiel R2, l'évaluateur doit étudier les risques de déni de service du réseau de gestion des accès et de la remontée d'alarmes. Il doit notamment vérifier qu'un tel déni de service ne puisse être aisément effectué depuis les zones publiques[20].

S'il mène une campagne de fuzzing, le CESTI devra décrire sa méthode (en particulier les règles de mutation et le volume de trafic envoyé). Le centre de certification pourra exiger que le script de fuzzing soit fourni si cette description n'est pas suffisante.

ii. Via les fonctions de gestion

Les fonctions de gestion jouent un rôle central dans le système. L'évaluateur sera donc attentif aux scénarios d'attaque du GAC ou de ses composants. Cela inclut typiquement, sans s'y limiter :

- la compromission des bases de données ou annuaires (clés, droits utilisateurs, etc.) ;
- la compromission du pilotage ou de la mise à jour distante de composants du système.

Les vecteurs privilégiés de ces scénarios seront en particulier :

- l'exploitation des interfaces du GAC[21] ;
- les faiblesses de cloisonnement entre les ressources du GAC et d'autres applicatifs[22] ;
- le cycle de vie des données de confiance[23].

iii. Via le réseau d'entreprise

L'évaluateur supposera par défaut que le système est connecté au réseau d'entreprise ; il s'attachera donc à étudier les interfaces exposées du système, mais aussi la dépendance du système à des données issues du réseau d'entreprise[24]. Si la cible de sécurité prévoit que le système soit déconnecté du réseau d'entreprise, l'évaluateur devra se prononcer sur la facilité d'emploi dans ce mode d'utilisation.

iv. Via Internet

Du point de vue du système, ce cas est le même que l'attaque depuis le réseau d'entreprise (voir section précédente), à plus forte raison si le système est connecté à Internet à travers le réseau d'entreprise. La cotation des vulnérabilités sera en revanche plus basse si un attaquant distant peut agir directement depuis *Internet* sans avoir besoin de rebondir depuis le réseau d'entreprise.

---

[20] Exemple : le rejeu d'une alerte d'arrachement d'un lecteur.

[21] Exemple : l'élévation de privilèges d'un utilisateur non privilégié depuis une interface de gestion - seuls les rôles les plus privilégiés (administrateur) sont nécessairement considérés comme « de confiance ».

[22] Exemple : si les hypothèses de la cible de sécurité autorisent l'installation de logiciels sur le même serveur que le logiciel de gestion du système, l'évaluateur vérifiera si ce serveur restreint les droits d'accès aux données sensibles du logiciel de gestion du système.

[23] Exemple : les mécanismes de révocation ou de renouvellement des clés utilisateur.

[24] Exemple : l'utilisation de certificats numériques issus d'une IGC d'entreprise.