SÉCURITÉ DES SYSTÈMES DE CONTRÔLE D'ACCÈS

COMPRENDRE LES RECOMMANDATIONS DE L'ANSSI

Qu'est-ce que l'ANSSI ?

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a été créée en 2009. Elle est rattachée au Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), autorité chargée d'assister le Premier Ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. C'est dans ce cadre que l'ANSSI agit pour assurer la cyberdéfense du pays en supervisant la protection des Secteurs d'Activité jugés d'Importance Vitale pour la France (SAIV).

→Mission

Afin de faire face aux nouvelles menaces, l'article 22 de la loi de programmation militaire du 18 décembre 2013 prévoit des mesures de renforcement de la sécurité des systèmes d'information que les Opérateurs d'Importance Vitale (OIV) de ces secteurs sont tenus de mettre en oeuvre.

L'ANSSI définit les règles applicables à ces mesures de protection renforcée et veille à leur strict respect. Ces obligations s'appliquent en priorité aux Systèmes d'Information d'Importance Vitale (SIIV), dont un des volets porte sur les systèmes de contrôle d'accès.

→ Les Secteurs d'Activité d'Importance Vitale

Un Secteur d'Activité d'Importance Vitale rassemble des activités et infrastructures jugées indispensables à la survie de la nation.

Il s'agit d'activités et d'infrastructures difficilement remplaçables et assurant la production et la distribution de biens et de services indispensables à la nation ou qui peuvent présenter un danger pour la population.

Le saviez-vous ?

12 Secteurs d'Activité d'Importance Vitale ont été identifiés.

- En France, 249 Opérateurs d'Importance Vitale (OIV) ont été désignés.
- Parmi ces OIV, 1 369 Points d'Importance Vitale (PIV) ont été identifiés et leur protection est une priorité.

Les Opérateurs d'Importance Vitale

Au sein des secteurs d'importance vitale, les Opérateurs d'Importance Vitale (OIV) assurent l'exploitation d'infrastructures elles-mêmes critiques. C'est pourquoi le SGDSN leur fixe des objectifs de sécurité. Ils sont tenus de coopérer à leurs frais, à la protection des établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste.

Les Points d'Importance Vitale

Les Points d'Importance Vitale sont des établissements, ouvrages ou installations qui fournissent les services et les biens indispensables à la vie de la nation au sein d'un OIV.

Ce sont les opérateurs eux-mêmes qui proposent la liste de leurs Points d'Importance Vitale qui peuvent être, notamment, des sites de production, des laboratoires, des centres de contrôle, des noeuds de réseau, des centres informatiques, etc. Un même opérateur peut donc être responsable de plusieurs Points d'Importance Vitale.

De même, il existe des Zones géographiques d'Importance Vitale (ZIV) comprenant des Points d'Importance Vitale (PIV) pouvant appartenir à plusieurs OIV.

La répartition des OIV par secteurs d'activités

Secteur	Transports	Militaires	Santé	Energie	Eau	Finances	Civiles	Médias	Espace	Judiciaires	Alimentation	Industrie
Nombre d'OIV*	68	36	22	21	16	15	10	9	7	6	5	5

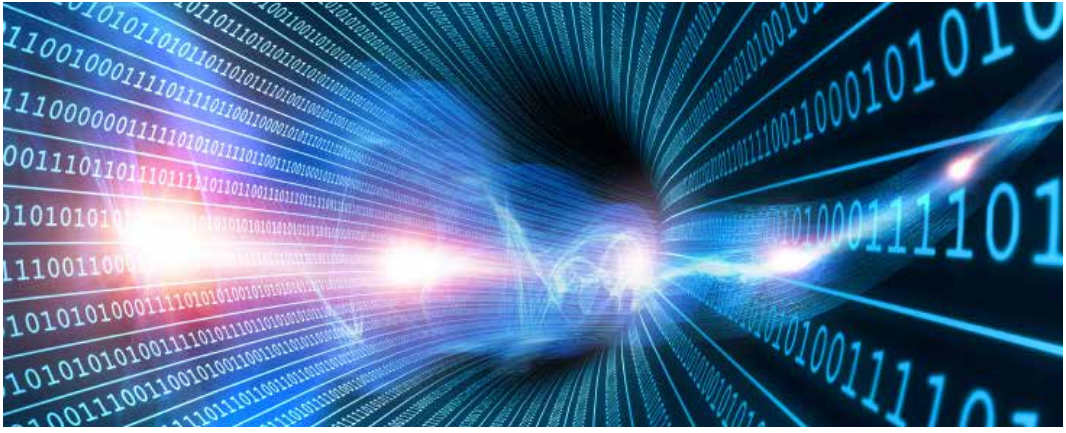
* OIV = Opérateur d'Importance Vitale

→ La législation en vigueur

Aux termes des articles L.1332-6-1 et suivants du Code de la Défense, les Opérateurs d'Importance Vitale sont tenus de mettre en oeuvre plusieurs types de mesures :

- Des règles de sécurité à la fois organisationnelles et techniques s'appliquant aux Systèmes d'Information d'Importance Vitale (SIIV).
- Des modalités d'identification des SIIV et de notification des incidents de sécurité affectant ces SIIV.

La France est le premier pays à s'appuyer sur la réglementation pour définir un dispositif efficace de cybersécurité de ses infrastructures critiques indispensables au bon fonctionnement et à la sécurité de la nation.



→ Les recommandations de l'ANSSI pour la sécurité des systèmes de contrôle d'accès

En ce qui concerne les systèmes de contrôle des accès physiques, l'ANSSI a résumé l'ensemble de ses recommandations dans un Guide « Sécurité des technologies sans-contact pour le contrôle des accès physiques ». Les principes fondamentaux qu'identifie ce document s'appliquent à des zones définies en fonction du type d'attaque potentielle.

Les niveaux de protection requis sont évalués selon une gradation de I à IV.

Le Guide détaille tout particulièrement :

- La protection des identifiants face au risque d'usurpation d'identité.
- L'architecture des systèmes face aux risques de cyberattaque.
- Le chiffrement des communications pour une sécurité de bout en bout.

Les 4 niveaux de sûreté des identifiants RFID :

Niveau	Description
I	L'identité présente sur le badge n'est pas protégée par chiffrement (exemple : badge à transpondeur 125 kHz, badge 13,56MHz utilisant le numéro de série). L'identifiant apparaît en clair et est de ce fait facilement clonable. Ce niveau ne présente aucune garantie de sécurité.
II	L'accès à l'identifiant du badge est protégé au moyen d'une clé permettant ainsi son authentification. Cette clé est secrète et est utilisée pour l'authentification du badge. Cette authentification repose sur l'usage d'une clé commune à l'ensemble des badges. Il s'agit ici du premier niveau de sécurité car en cas de corruption de la clé, l'accès à l'ensemble des identifiants serait rendu possible.
III	L'accès à l'identifiant du badge est protégé au moyen d'une clé unique propre à chaque badge. L'authentification repose sur l'usage d'une clé calculée à partir d'une clé maîtresse. Dans ce cas, la corruption de la clé du badge n'affecte pas les autres badges.
IV	Idem Niveau III + authentification du porteur par la saisie d'un code mémorisé ou au moyen d'une donnée biométrique.

L'application des niveaux de sûreté II à IV recommandés par l'ANSSI exige l'emploi de badges équipés de puces dotées de fonctions de chiffrement. La certification de la puce aux critères communs EAL 4+ est un gage supplémentaire de sécurité. Aujourd'hui, le badge Mifare® DESFire EV1 s'est imposé comme la référence en ce domaine.

Le saviez-vous ?

Acquérir des badges supportant la mise en œuvre de mécanismes de chiffrement ne suffit pas.
Il faut activer correctement ces mécanismes, faute de quoi les badges ne seront utilisés qu'en identification, et pourront donc être clonés.
Les clés de chiffrement utilisées dans ce contexte peuvent être de complexité variable. Elles sont la propriété et le secret de l'organisation qui les met en oeuvre. Elles nécessitent de ce fait des moyens organisationnels et techniques clairement définis pour assurer leur diffusion sécurisée de bout en bout.

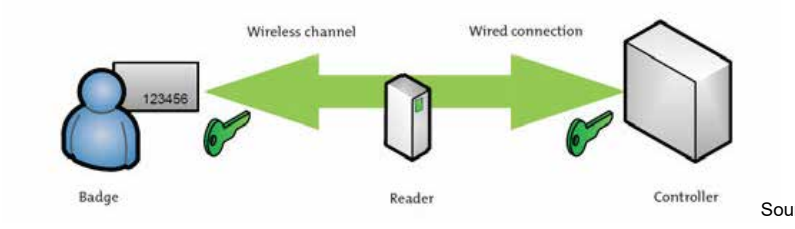
Les architectures des systèmes de controle d'accès

La mise en oeuvre des niveaux de sûreté II à IV nécessite l'utilisation d'une architecture en adéquation avec le niveau de protection requis. En effet, de la même manière que les accès à des identifiants sont protégés par des clés, il faut sécuriser la diffusion et le stockage de ces clés. Celles-ci sont, en fonction des architectures, situées soit dans le lecteur soit dans le contrôleur.

L'ANSSI définit 4 types d'architectures (numérotées de 1 à 4) mais ne recommande que l'architecture n° 1.

Architecture n° 1, hautement recommandée

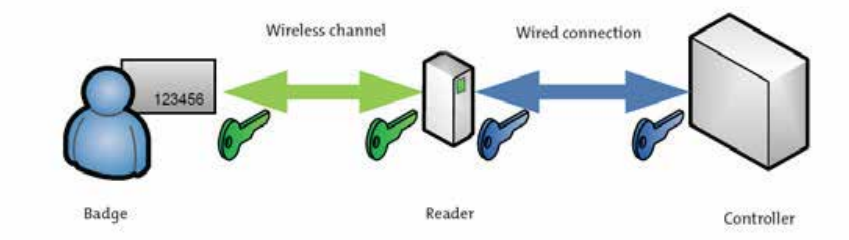
Le badge sécurisé s'identifie et s'authentifie directement auprès du contrôleur (UTL) situé en zone sécurisée. La tête de lecture transmet les messages sans les modifier et ne participe pas au chiffrement. Elle est dite « transparente ».
Cette architecture est hautement recommandée par l'ANSSI car la tête de lecture ne contient aucun élément secret et est de ce fait inattaquable. L'UTL demande de son côté une attention particulière pour la protection des clés de chiffrement qui devront être stockées dans un module de sécurité : SAM (Secure Access Module), physique ou virtuel. La certification CSPN délivrée par l'ANSSI pour cette architecture complète en garantit la conformité.



Source : ANSSI

Architecture n° 2 (acceptable sous conditions)

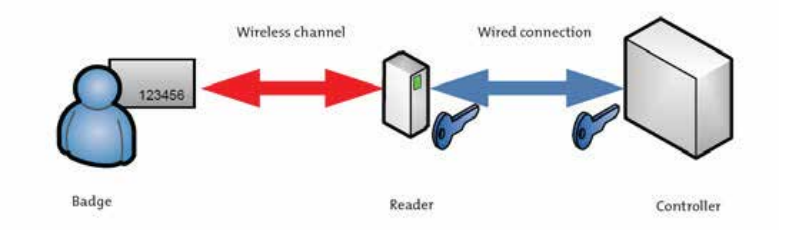
Le badge sécurisé s'identifie et s'authentifie au niveau de la tête de lecture. Cette dernière doit avoir une liaison sécurisée avec authentification et chiffrement pour garantir la protection des échanges d'information avec le contrôleur (UTL).
La tête de lecture, située hors de la zone de sécurité, renferme à la fois les secrets permettant l'authentification de la carte et les secrets permettant de protéger la liaison filaire.
Cette architecture ne peut être acceptée que si la tête de lecture et l'UTL ont fait l'objet d'une étude de sécurité approfondie garantie par la Certification de Sécurité de Premier Niveau (CSPN). La protection de la liaison filaire du côté de l'UTL est un point de vigilance fort car elle doit être garantie à la fois par le fabricant de l'UTL et celui de la tête de lecture.
Cette architecture demande la gestion de plusieurs jeux de clé de sécurité et est de ce fait plus contraignante et pour l'installateur et pour l'exploitant. La mise à la clé du lecteur nécessite la plupart du temps la diffusion des clés à un tiers et multiplie le risque de faille de sécurité.



Source : ANSSI

Architecture n° 3 (fortement déconseillée)

Le badge - non sécurisé - s'identifie directement auprès du contrôleur (UTL). Le badge peut être cloné, y compris hors du site, ce qui rend sans intérêt la protection filaire. Il ne peut servir que pour l'identification.

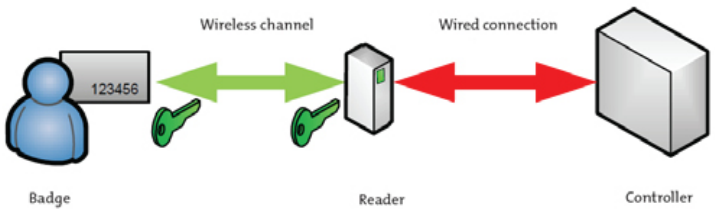


Source : ANSSI

Architecture n° 4 (fortement déconseillée)

Le badge sécurisé s'identifie et s'authentifie avec la tête de lecture. Cette dernière transmet de manière non protégée l'identité au contrôleur (UTL).

L'authentification peut être contournée par une attaque sur la liaison filaire en zone exposée.



Source : ANSSI

→ Glossaire

Identification d'un usager

L'identification permet de communiquer et de traiter l'identité de l'usager.
Avec la technologie sans contact, l'identification se fait par la présentation du badge de l'usager sur un lecteur d'accès.

Authentification d'un usager

L'authentification permet d'apporter la preuve de l'identité d'un usager.

Lorsque l'usager a été identifié, un second élément est alors utilisé : ce que le porteur sait (code connu du porteur) ou ce qu'il est physiquement (caractéristique biométrique).

→ La procédure de certification ANSSI-CSPN

La CSPN

La certification permet d'attester par une tierce partie indépendante et impartiale qu'un produit atteint, à un instant donné, un niveau de sécurité représenté par les services de sécurité qu'il offre et sa résistance à un niveau d'attaques donné : en France, quel que soit le type d'évaluation, la certification s'appuie systématiquement, outre des vérifications de conformité, sur des tests d'intrusion pour déterminer le niveau de sécurité réellement atteint par le produit. (Source : ANSSI)

Cible de sécurité

L'évaluation peut porter sur tout ou partie du produit. Lors de l'évaluation, la cible de sécurité doit être spécifiée. Cette cible définit le périmètre de composants qui sera évalué et donc certifiable.

Objectif de l'évaluation

Le but de la procédure d'évaluation est de permettre à un centre agréé de vérifier la conformité du produit avec ses spécifications, de déterminer l'efficacité de ses fonctions de sécurité et de consigner les résultats des tests dans un rapport technique d'évaluation (RTE).

L'organisme certificateur (l'ANSSI) utilise alors ce rapport pour décider s'il accorde ou non la certification CSPN au produit.

→ Le système de contrôle d'accès SMI de Fichet

Fichet, constructeur de référence dans le domaine du contrôle d'accès physique, a placé la certification CSPN au coeur de sa démarche d'Entreprise. Sa volonté est de mettre à disposition du marché des systèmes ouverts, pérennes et évolutifs destinés à contrer efficacement l'évolution de la menace.

Le Système de Management Intégré de la sûreté (SMI) de Fichet figure parmi les très rares solutions de contrôle d'accès certifiées CSPN dans la catégorie « Identification, Authentification et Contrôle d'accès ».

Il répond à l'ensemble des exigences de l'ANSSI en la matière :

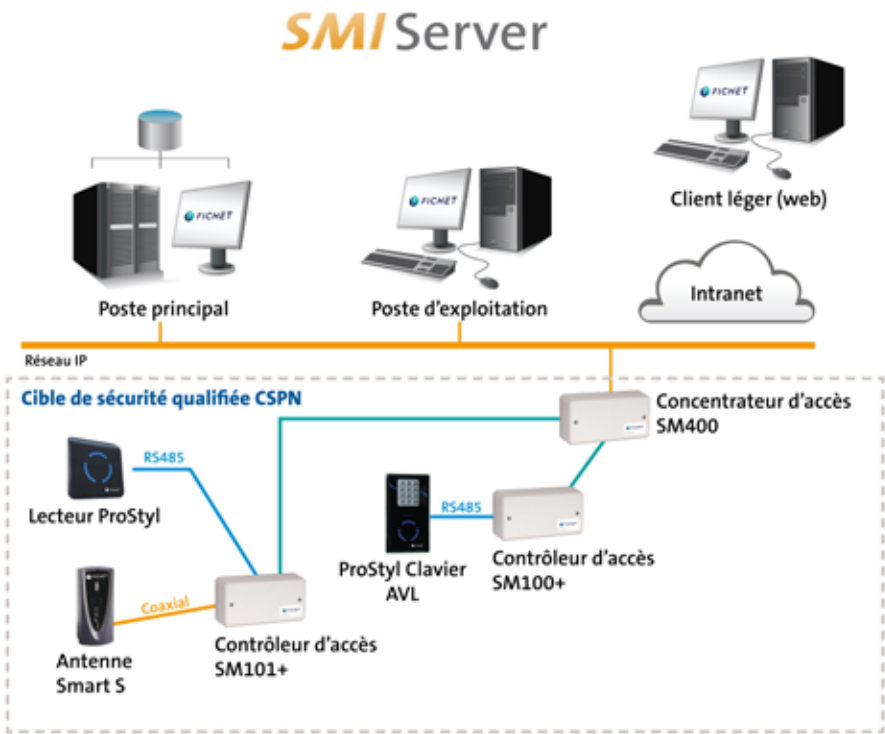
- Architecture n° 1 hautement recommandée.
- Compatibilité avec les niveaux de sûreté I à IV.
- Chiffrement des liaisons de bout en bout.
- Procédure sécurisée de mise à la clé des contrôleurs.

Le saviez-vous ?

SMI, c'est aussi :

- Un superviseur de sûreté entièrement paramétrable.
- La gestion des alarmes et l'aide à la décision.
- Des outils de qualification contextuels.
- Des fonctions vidéos interactives avancées.
- Une plateforme d'intégration puissante et ouverte.
- ...

Cible de sécurité



Pour en savoir plus sur la certification Fichet SMI Version CSPN 01-01 : http://www.ssi.gouv.fr/entreprise/certification_cspn/Fichet-smi-version-cspn_01-01/

FICHET

www.fichetgroup.fr

Fichet se réserve le droit de modifier sans préavis ses produits et leurs caractéristiques. Les illustrations du présent document ne sont que des exemples d'installation et peuvent donc ne pas correspondre à la version standard du produit.