PREMIER MINISTRE
Secrétariat Général de la Défense et la Sécurité Nationale
Agence Nationale de Sécurité des Systèmes d'Information

GUIDE

SECURITE DES TECHNOLOGIES SANS-CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES

Table des matières

1 Introduction

1.1 Contexte

Plusieurs failles de sécurité affectant les technologies sans contact sont avérées. Un groupe de travail interministériel, animé par l'Agence nationale de sécurité des systèmes d'information (ANSSI[1]) a évalué que les conséquences de ces failles étaient particulièrement préoccupantes lorsque les technologies sans contact étaient utilisées dans les systèmes de contrôle des accès physiques.

Face à ce constat, l'Agence a estimé utile de publier un guide sur la sécurité des technologies sans-contact pour le contrôle des accès physiques. Ce guide explique en quoi les systèmes de contrôle d'accès doivent être considérés comme des systèmes d'information à part entière, relevant du périmètre de la Direction des Systèmes d'Information (DSI), où doivent s'appliquer les règles élémentaires de l'hygiène informatique.

Ce guide se limite aux aspects d'architecture et de sécurité logique propres aux systèmes de contrôle d'accès utilisant des technologies sans contact. L'ANSSI s'est associée au CNPP[2] - Centre national de prévention et de protection – pour mener une réflexion intégrant l'ensemble des éléments qui composent ces systèmes de contrôle.

Ce guide est ainsi complémentaire du référentiel CNPP intitulé « APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation », qui traite plus particulièrement des aspects physiques pour les différentes technologies de systèmes de contrôle des accès, tels que la résistance à l'effraction ou encore le contournement de l'obstacle. Les deux documents présentent en commun le Tableau 1 : Les quatre niveaux de sûreté, qui a été conçu en concertation.

1.2 Objectifs du guide

Ce guide se veut une aide à la décision quant au choix d'un système de contrôle d'accès sans contact, et propose les bonnes pratiques à déployer pour sa mise en œuvre.

Il fournit des recommandations permettant d'assurer la mise en place d'un système de contrôle d'accès reposant sur les technologies sans contact en conformité avec un niveau de sécurité satisfaisant. Ces recommandations s'appliquent aussi bien à des systèmes de contrôle d'accès « mono-sites », ou des systèmes « multi-sites », dont la gestion est centralisée.

Pour les sites où des technologies sans contact sont déjà déployées, ce guide donne aux gestionnaires des éléments pour effectuer une vérification de leur niveau de sécurité et pour s'assurer que les bonnes pratiques sont appliquées.

De plus, ce guide accompagne les choix d'évolution technologique en détaillant les recommandations à suivre pour que le niveau de sécurité global du site soit cohérent avec le niveau de sécurité de la technologie utilisée.

L'objectif de ce guide n'est cependant pas d'imposer une architecture ou une solution technique. Il n'a pas non plus vocation à servir de cible de sécurité pour les produits de contrôle d'accès sans contact.

1.3 Public cible

Ce guide s'adresse :

- aux chefs de projet ou personnes en charge de la mise en place d'un système de contrôle d'accès sans contact, que ce soit dans une entreprise privée ou un organisme public ;
- aux acheteurs, qui pourront imposer dans leurs appels d'offre les exigences détaillées en chapitre 5 afin de les rendre contraignantes pour le fournisseur ;
- aux installateurs ou intégrateurs, qui pourront tenir compte du contenu de ce guide afin de proposer des services adaptés ;
- aux exploitants, qui s'intéresseront aux aspects liés à l'exploitation et la maintenance du système.

Les objectifs de ces différents acteurs n'étant pas les mêmes, le tableau ci-dessous permet d'identifier, pour chacun d'entre eux, les chapitres qui les concernent plus particulièrement :

[1] Site Internet de l'ANSSI : http://www.ssi.gouv.fr
[2] Centre national de prévention et de protection – http://www.cnpp.com

Acteurs	Chapitres recommandés
Chef de projet Personnes en charge de la mise en place d'un système de contrôle d'accès sans contact.	Chapitre 2 : Fondements du contrôle d'accès Chapitre 3 : Expression de besoins Chapitre 4 : Choix du système
Acheteurs	Chapitre 5 : Spécifications
Installateurs Intégrateurs	Chapitre 2 : Fondements du contrôle d'accès Chapitre 4 : Choix du système Chapitre 5 : Spécifications Chapitre 6 : Installation du système
Exploitants	Chapitre 7 : Exploitation du système

2 Fondements du contrôle d'accès

2.1 Définition

Un système de contrôle des accès physiques est un dispositif ayant pour objectif de filtrer les flux d'individus souhaitant pénétrer à l'intérieur d'un site, d'un bâtiment ou d'un local. Il est constitué de moyens permettant d'autoriser les entrées et sorties de zones sensibles aux seules personnes qui ont le droit d'y accéder.

Un système de contrôle d'accès assure trois fonctions primaires :

- l'identification et l'authentification ;
- le traitement des données[3] ;
- le déverrouillage.

Ces fonctions sont assurées en chaque point où l'accès est contrôlé.

Dans le cas d'un système de contrôle d'accès utilisant des technologies sans contact, quatre éléments support principaux interviennent :

- le badge (ou support similaire)[4] ;
- le lecteur (tête de lecture) ;
- l'unité de traitement local (désignée par UTL, également connue sous le nom d'unité de traitement et de contrôle) ;
- le serveur de gestion du système présenté en 4.1.6.

En outre, il convient de prendre en considération la sécurité des liaisons filaires entre les éléments, ainsi que la sécurité du serveur de gestion du système de contrôle d'accès (également appelé UTS – Unité de Traitement de Supervision, ou GAC – Gestion des Accès Contrôlés) et des postes de travail utilisés pour la programmation.

2.2 La phase d'identification et d'authentification

Les notions d'identification et authentification définies dans ce guide sont conformes aux recommandations de l'Agence nationale de la sécurité des systèmes d'information[5] telles qu'exprimées dans le Référentiel général de sécurité, disponible sur son site Internet. Elles diffèrent des définitions émises dans la norme NF EN 50133 « Systèmes d'alarme - Systèmes de contrôle d'accès à usage dans les applications de sécurité ».

Pour mémoire :

S'identifier, c'est le fait de communiquer une identité.

S'authentifier c'est apporter la preuve de son identité : c'est donc un élément complémentaire à l'identification.

Dans le contexte des systèmes de contrôles d'accès, et en fonction de la technologie choisie, la phase dite d'identification/d'authentification peut se réduire à l'identification du badge, ou à l'identification et l'authentification du badge seulement.

- identification

  Dans un système reposant sur une technologie sans-contact, l'identification est la présentation d'un badge à un lecteur.

- authentification du badge

  L'authentification du badge consiste à prouver qu'il est valide.

  Pour un système de contrôle d'accès reposant sur des technologies sans-contact, l'authentification du badge se fait le plus souvent par un échange cryptographique permettant au badge de prouver qu'il détient des éléments secrets sans les révéler. Si les fonctions

[3] La fonction de traçabilité des accès est assurée dans le cadre du traitement des données.
[4] Par soucis de facilitation de la lecture, le terme « badge » sera utilisé de façon générique pour désigner tout type de support.
[5] http://www.ssi.gouv.fr

cryptographiques sont suffisamment robustes, il n'est pas possible de cloner un tel badge tant que les éléments secrets restent protégés. Néanmoins, le badge, support physique, peut être volé. Le processus d'authentification d'une carte et de transmission sécurisée de l'identifiant est présenté en Annexe 1 : Processus d'authentification d'une carte et de transmission sécurisée de l'identifiant.

- authentification du porteur

Le badge étant préalablement authentifié, il s'agit pour le porteur du badge de prouver qu'il en est le détenteur légitime.

L'authentification du porteur se fait par l'usage d'un second élément[6] sélectionné parmi ce que l'on est et ce que l'on sait. Elle peut se faire par exemple par la saisie d'un mot de passe que seul le détenteur légitime du badge connaît ou par l'usage de la biométrie[7].

2.3 Traitement des données

Le traitement de données est assuré en premier lieu par l'unité de traitement local (UTL). Cette unité assure la gestion de toutes les demandes d'accès, compare ces demandes par rapport à un ensemble de droits d'accès stockés dans sa base de données, et délivre les commandes de libération des verrouillages.

Le serveur de gestion du système :

- centralise les journaux événements ;
- remonte les événements au gestionnaire ;
- héberge la base de données centrale, tenue à jour (droits, utilisateurs, groupes, badges, etc.) ;
- pilote l'ensemble des UTL en leur transmettant la base de données nécessaire à leur traitement des demandes d'accès.

2.4 Verrouillage et déverrouillage

Le dispositif de verrouillage permet de réaliser le blocage mécanique du point d'accès pour empêcher le passage des personnes non autorisées. Le contrôle d'accès autorise le déverrouillage.

Dans le cadre de l'analyse des risques, il conviendra de prendre en compte les situations dégradées (coupure électrique) et les cas d'ouverture automatique (incendie). Ces deux questions sont traitées dans le chapitre 7.3, « Procédures d'exploitation particulières ».

[6] Le badge constitue le premier élément : ce que l'on a.

[7] La biométrie est assimilable à une méthode d'identification, car les éléments biométriques ne sont ni secrets, ni révocables. Elle peut donc se substituer au badge en tant que moyen d'identification, mais en aucun cas comme moyen d'authentification. Elle peut toutefois être utile pour authentifier le porteur, en association avec un badge stockant les éléments biométriques permettant la comparaison, dont le badge assure l'intégrité. Ce compromis reste d'une sécurité inférieure au mot de passe, qui peut être gardé secret, et qui est répudiable.

3 Expression de besoins

Pour bien cerner les besoins relatifs au contrôle des accès physiques, il est nécessaire en premier lieu d'établir une cartographie précise de tous les éléments qui détermineront les caractéristiques du système de contrôle mis en place. Parmi ces éléments, on retrouve entre autres :

- les sites à protéger, et les zones qui les composent ;
- les biens essentiels[8] et biens supports à protéger ;
- les flux de circulation entre ces zones ;
- l'organisation (responsabilités, acteurs, processus).

Ces aspects ne seront évoqués que sommairement dans ce guide. Les lecteurs qui souhaiteraient accéder à plus d'information peuvent se référer au référentiel « APSAD D83 – Contrôle d'accès – Document technique pour la conception et l'installation »[9].

3.1 Identification des sites

L'identification détaillée des sites est une étape importante de la réflexion préalable à la mise en place d'un système de contrôle d'accès. Cette réflexion permet de clarifier les contraintes qui pèsent sur le projet et de disposer des éléments nécessaires à la rédaction des appels d'offre. Les sites à contrôler doivent donc être référencés de manière exhaustive, en prenant en compte leurs particularités.

Pour chaque site, les éléments suivants doivent être considérés :

- nom du site (pour l'identification) ;
- adresse (pour la géolocalisation) ;
- nature du site (immeuble entier, quelques étages seulement, quelques pièces uniquement) ;
- dédié ou partagé avec d'autres organismes ou entreprises ;
- services à proximité (police, pompiers, etc.) ;
- risques naturels (zone inondable, sismique, etc.) ;
- nombre de personnes actuel et potentiel.

3.2 Identification des biens essentiels et biens supports à protéger

Ce guide ayant pour vocation de traiter du système de contrôle des accès physiques du point de vue de la sécurité des systèmes d'information, nous considèrerons qu'un bien essentiel est une ressource immatérielle, telle que de l'information, ou un processus. Dans une approche plus large, il pourrait s'agir de toute ressource nécessaire à la réalisation des objectifs de l'organisme. Dans un tel cas, par extension, il serait possible de considérer que des ressources matérielles sont des biens essentiels.

Les biens essentiels s'appuient sur des biens supports qui en assurent le traitement, le stockage et la transmission. Ainsi un serveur de calcul n'est pas un bien essentiel mais un bien support, de même que les locaux, les systèmes informatiques, et les différents équipements. Le bien essentiel est le processus de calcul, et le serveur est le bien support qui permet l'exécution du processus.

Il est recommandé de lister les biens essentiels à protéger, et les biens supports sur lesquels ils s'appuient, pour déterminer les ressources dont il convient de contrôler les accès physiques. L'ANSSI publie une méthode de gestion des risques apportant des recommandations pour l'analyse exhaustive des biens essentiels et des biens supports : la méthode EBIOS[10].

3.3 Identification de zones

Après avoir réalisé l'inventaire des biens essentiels, des biens support, et de leur localisation, il est possible de distinguer des zones avec des niveaux de sensibilité différents au sein des sites à protéger.

[8] Il est utile de faire une distinction entre les biens essentiels qui, dans un système d'information, sont des biens immatériels (informations ou processus utiles à la réalisation des missions de l'organisme), des biens supports dont ils dépendent pour le traitement, le stockage ou la transmission.
[9] CNPP éditions ; http://www.cnpp.com/
[10] Téléchargeable gratuitement sur http://www.ssi.gouv.fr/ebios

Il est recommandé d'établir une échelle précise et explicite des niveaux de sensibilité, avec leurs définitions associées.

La numérotation à partir de zéro est tout-à-fait indiquée pour cet usage, le niveau zéro étant alors la zone considérée comme publique, à l'intérieur de la limite de propriété.

Les niveaux suivants sont les zones sous contrôle, entourées de barrières physiques comprenant un nombre restreint de points d'accès, et situées dans l'enceinte des sites ou des bâtiments. Les niveaux les plus élevés sont les zones névralgiques. Les zones où seront situés les éléments du système de contrôle d'accès (serveur de gestion du système, et postes de travail clients) devront être également définies avec le niveau de sensibilité adéquat.

Les sites à protéger doivent être découpés en zones classées par niveaux de sensibilité selon l'échelle préalablement conçue. Ces zones n'ont pas à être découpées selon la configuration physique existante des lieux, mais bien selon leur sensibilité réelle : un tel projet peut soulever la nécessité de conduire des travaux ou des réorganisations des cloisons, des sites et des bâtiments afin que la sécurité physique soit optimisée voire même rendue possible.

Sur le plan de bâtiment ci-dessous ont été représentées trois zones de niveaux de sensibilité différents :

- zone semi-publique (verte), accessible à tout le monde mais destinée aux visiteurs et placée sous vidéo-surveillance ;
- zone de bureaux (orange), accessible aux employés et aux visiteurs autorisés au moyen d'un badge et d'un contrôle visuel au niveau de la réception ;
- salle serveurs (rouge) accessible aux seuls employés autorisés et aux visiteurs accompagnés au moyen d'un badge et d'un code.

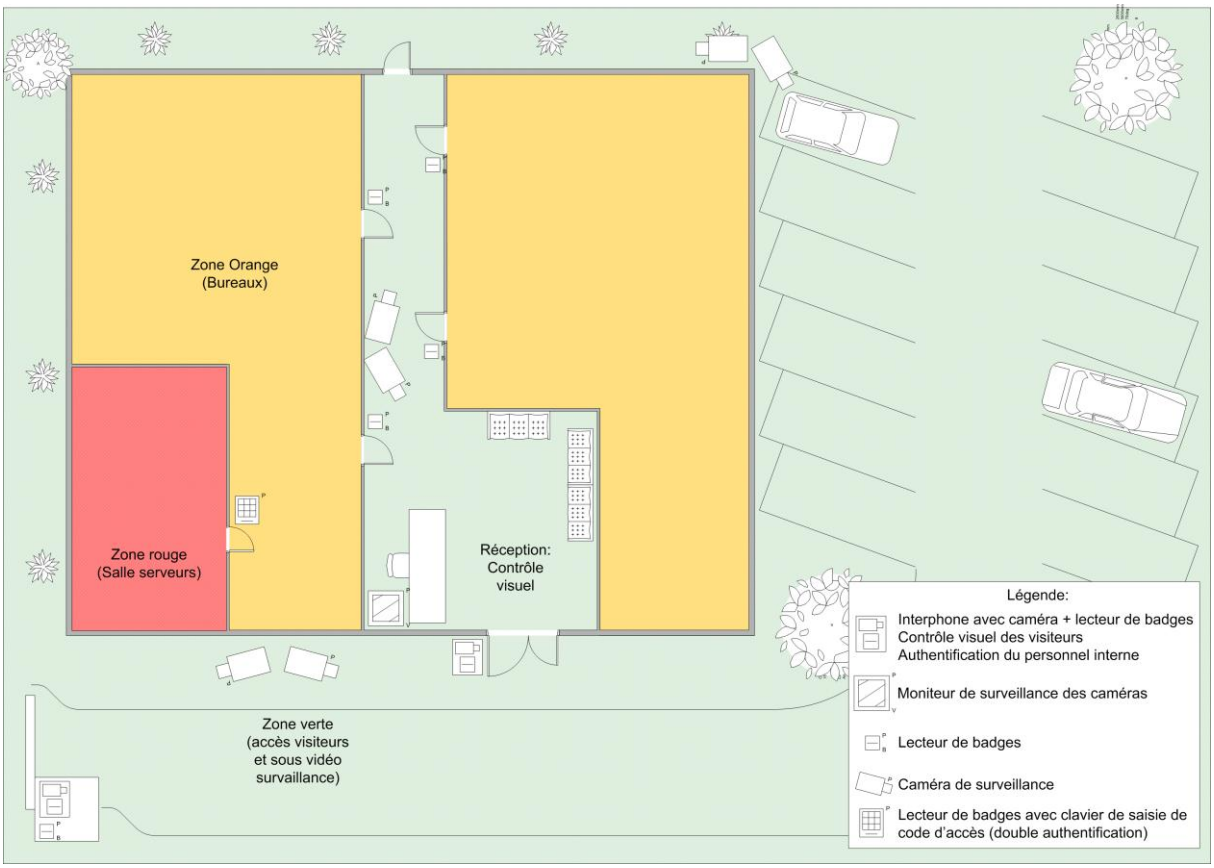


Figure 1 : Exemples de zones

3.4 Niveau de sûreté et types de menaces

Le niveau de sûreté des équipements et des installations de contrôle des accès physiques correspond à un niveau de résistance à l'effraction et à la fraude. Le niveau de sûreté découle directement du type de menaces redouté pour chaque niveau de sensibilité des zones précédemment définies.

Ces niveaux de sûreté et types de menaces ont été définis en lien avec le CNPP. Ce même tableau est reproduit dans le référentiel « APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation » :

Menaces potentielles			**Niveaux de sûreté**
Qui ?	**Quels moyens ?**	**Quelles connaissances ?**	
Franchissement « naturel » d'un point d'accès			
Pénétrations involontaires ou de curieux	Pas de matériel ou matériel basique (marteau léger, téléphone portable…)	Pas de connaissance	**I**
Franchissement par attaque mécanique et/ou logique « simple »			
Pénétrations préméditées de personnes faiblement équipées	Matériel et méthode obtenus dans le commerce ou sur Internet.	Connaissance basique du système acquise au travers de documents publicitaires ou technico-commerciaux émis par le fabricant ou les distributeurs.	**II**
Franchissement par attaque mécanique et/ou logique « évoluée »			
Pénétrations préméditées de personnes initiées et équipées.	Matériel ou maquette électronique spécifique facilement réalisable.	Connaissances recueillies à partir de l'examen d'un dispositif.	**III**
Franchissement par attaque mécanique et/ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées.	Matériel comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.	Connaissances sur la conception et l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant.	**IV**

Tableau 1 : Les quatre niveaux de sûreté

Ce tableau ne prend pas en compte l'impact de filtrages réalisés par des moyens humains ou non, tels que de la surveillance humaine ou de la vidéo surveillance 24h/24, et qui sont susceptibles de réduire le besoin de sûreté des équipements et des installations de contrôle des accès physiques nécessaires.

3.5 Flux de circulation des individus

L'analyse des flux de circulation des individus permet de connaître les besoins de chaque point d'accès à contrôler. Il s'agit de répondre aux questions : Qui ? Quand ? Comment ? Combien ?

Il est pour cela utile de définir :

- les différentes catégories de personnel autorisées (personnel interne, intérimaires, agents de surveillance, prestataires de services, clients, visiteurs, services d'urgences, etc.) ;
- les plages horaires ;
- le type de passage à contrôler (simple porte, sas, entrée de véhicules) ;
- les exigences de circulation particulières et contraintes spécifiques (sorties de secours) ;
- la quantité prévisionnelle de passages.

Trois exemples de flux physiques ont été représentés sur le plan de bâtiment ci-dessous, montrant les principales personnes extérieures intervenant au sein des locaux et leurs déplacements autorisés.

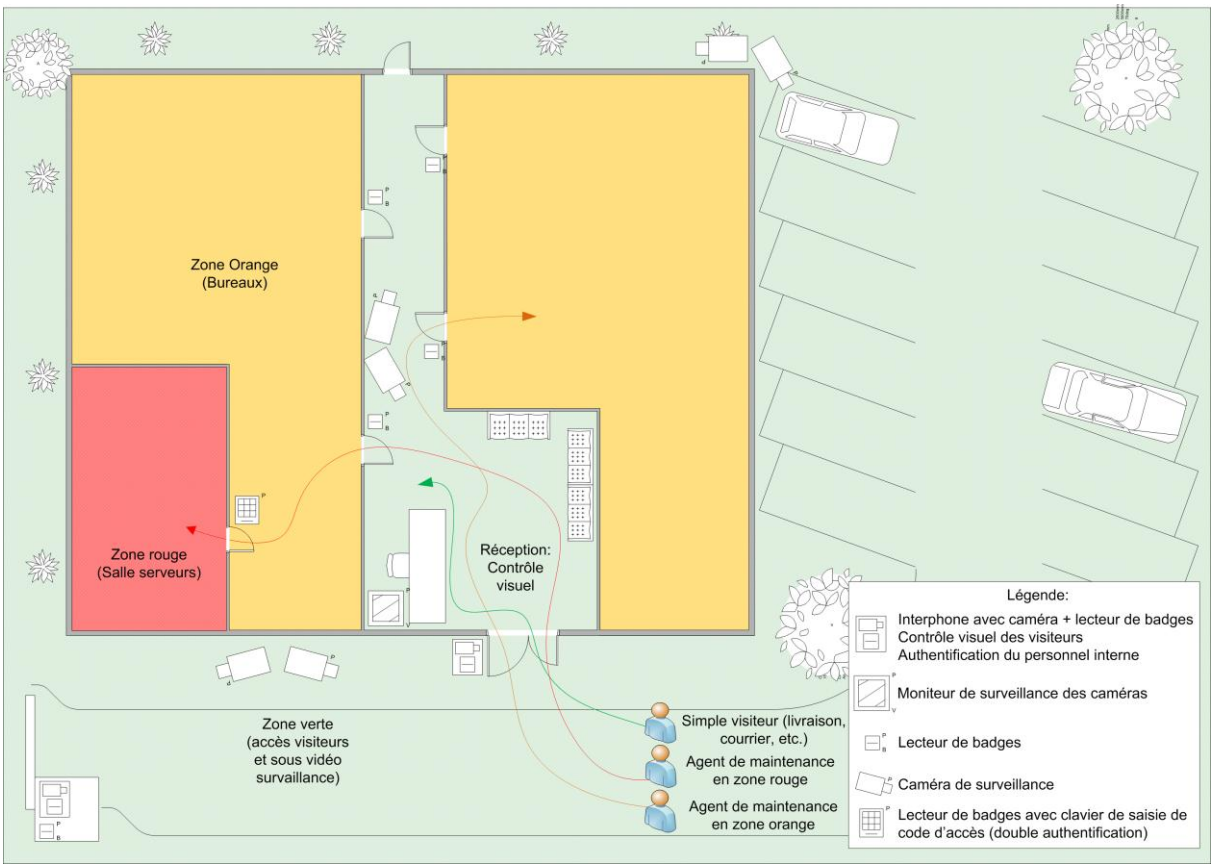


Figure 2 : Exemples de flux physiques

3.6 Identification des acteurs

Les différents acteurs et responsables doivent être clairement identifiés. On distingue plusieurs types d'acteurs pouvant intervenir dans les processus organisationnels de gestion des accès physiques :

- les demandeurs (service de gestion des ressources humaines, managers, etc.) qui font les demandes d'attribution de badges et droits associés ;
- les responsables de validation (responsables de sites ou de zones), qui valident ou non les différents droits demandés ;
- les informés, qui ont connaissance des attributions et révocations de badges et de droits à différentes fins ;
- les opérateurs du système de contrôle des accès physiques ;
- les opérateurs de sauvegarde du système ;
- les opérateurs d'exploitation des journaux d'événements du système ;
- les mainteneurs des matériels physiques ;
- les mainteneurs applicatifs[11] ;
- les utilisateurs finaux, à qui sont attribués les badges.

Selon la situation, plusieurs rôles peuvent être assurés par les mêmes personnes. Il convient de s'assurer que ce cumul ne confère pas tous les droits à une seule personne et que des mécanismes d'approbation et de contrôle indépendants sont mis en place et respectés.

[11] Une attention toute particulière doit être portée à la sécurité du système lorsqu'il est fait appel à de la télémaintenance. L'ANSSI a publié un guide sur l'infogérance : http://www.ssi.gouv.fr/infogerance

3.7 Processus organisationnels

Les flux organisationnels doivent être clairement déterminés dès l'expression des besoins. Il s'agit de représenter les échanges nécessaires entre les acteurs pour réaliser un objectif particulier. Ces échanges peuvent être informatisés ou non. On distingue communément les processus suivants :

- demande de badge ;
- délivrance de badge ;
- révocation de badge ;
- modification de droits.

Des exemples types de ces processus peuvent être consultés en Annexe 3, « Exemple de processus organisationnels ».

3.8 Continuité de service

Il est nécessaire d'avoir une réflexion sur le niveau de continuité de service souhaité : tolérance aux pannes, autonomie en cas de coupure électrique, délais de remplacement du matériel dans le contrat de maintenance, etc. Le besoin doit être exprimé de manière rationnelle afin de ne pas engendrer des coûts inutilement démultipliés.

3.9 Interconnexions

Les interconnexions avec d'autres systèmes (vidéo surveillance, système de gestion des ressources humaines, etc.) doivent être référencées et/ou exprimées au préalable car elles ont un impact sur le projet de mise en place d'un système de contrôle d'accès. La nature de ces interconnexions doit être détaillée afin que les réponses aux appels d'offre soient cohérentes en regard des systèmes existants.

3.10 Badges multi-usages

Dans certaines circonstances, il peut s'avérer utile de mutualiser les usages sur un même badge. Il est ainsi envisageable d'ajouter sur le badge, en plus de la puce utilisée pour le contrôle d'accès, une seconde puce pour s'authentifier sur le système d'information de l'organisme. D'autres usages (tels que le porte-monnaie électronique) peuvent être envisagés selon le même principe.

En cas de mutualisation des usages sur un badge unique, il convient de bien analyser les solutions existantes pour limiter les risques, en cas de perte ou vol du badge notamment. L'objectif devra être que la compromission d'un élément ne doit pas entrainer la compromission des autres. Chaque usage doit donc être porté par un composant indépendant.

3.11 Contraintes règlementaires

Certaines zones protégées sont concernées par des réglementations particulières qui impacteront les caractéristiques du système de contrôle des accès. Un aperçu des principales règlementations peut être consulté en Annexe 4 – « Contraintes réglementaires ».

Lorsque le besoin a été correctement défini, il devient dès lors possible de choisir un système adapté au contexte et aux enjeux de l'organisme.

4 Choix du système

Le choix d'un système nécessite de prendre en compte plusieurs critères, liés à sa conception même (architecture et sécurité des éléments support) et aux contraintes réglementaires.

4.1 Sécurité des éléments supports

Afin de mieux visualiser le positionnement des différents éléments support dans l'architecture générale d'un système de contrôle des accès physiques, un schéma est disponible en Annexe 1.

4.1.1 Badges : niveaux de sûreté, résistance aux attaques logiques.

Le Tableau 2 ci-dessous établit le lien entre les niveaux de sûreté et des niveaux de résistance aux attaques logiques.

Niveau de sûreté	Résistance aux attaques logiques[12]	Méthode	Technologie	Caractéristiques
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement clonable
II	L1	Authentification du badge.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clef commune ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
III	L2	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clef dérivée d'une clef maîtresse ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
IV	L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clef dérivées.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clef dérivée d'une clef maitresse ; Algorithmes et protocoles d'authentification connus et réputés (3DES, AES).

Tableau 2 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques

Les badges ne doivent avoir pour seule et unique information enregistrée qu'un numéro d'identification. Il est déconseillé d'y stocker d'autres informations. Toute autre information d'authentification mémorisée supplémentaire (mot de passe, code PIN), doit être stockée au niveau du serveur de gestion du contrôle d'accès ou des unités de traitement local.

A noter : pour répondre aux principes exposés ici, une demande d'autorisation devra être faite selon les procédures complètes de la CNIL : en cas d'usage de la biométrie il faut noter que la CNIL[13] facilite certaines formalités de demande d'autorisation, mais uniquement lorsque l'information est stockée sur le badge[14]. Ces procédures visent la protection des données personnelles, et non pas

[12] Le risque de substitution par création d'un badge valide est pris en compte en tant qu'attaque logique.

[13] Commission Nationale de l'Informatique et des Libertés - http://www.cnil.fr/

[14] C'est le cas notamment pour l'emploi de l'empreinte digitale lorsqu'elle est exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-008)

celle du système de contrôle d'accès. La procédure simplifiée impose des conditions contraires aux principes exposés dans ce document, qui déconseille le stockage d'informations sur le badge.

>> Il est recommandé que les badges soient visuellement les plus neutres possibles. Ils ne doivent pas indiquer :

- **d'informations sur l'entreprise (nom, adresse) ;**
- **d'informations sur le porteur (nom, prénom, poste), en dehors de sa photo ;**
- **les accès qu'ils permettent.**

Ils peuvent, en revanche, indiquer visuellement un numéro de traçabilité (ex. : XXX sur la Figure 3 ci-dessous), différent du numéro d'identification (ex. : YYY sur la Figure 3 ci-dessous), ne révélant rien sur la nature du badge. Ce numéro de traçabilité pourra être utilisé à des fins d'administration par le gestionnaire du système. La photographie est tolérée car elle permet de vérifier rapidement que le badge appartient bien au porteur.

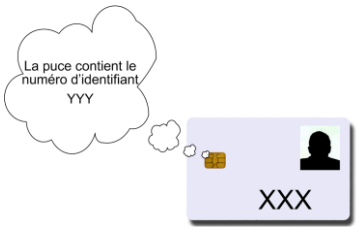


Figure 3 : Exemple de badge

En ce qui concerne les types de badges, il est regrettable de noter le peu d'options disponibles au moment de la rédaction de ce guide (4e trimestre 2012). Un certain nombre de supports ne permettront que l'identification (de type puce RFID[15], comparable aux antivols dans les magasins). D'autres disposent de fonctions cryptographiques qui permettent une authentification (de type carte à puce, comparable aux cartes de paiement bancaire).

Certaines technologies de carte d'accès qui font appel à des mécanismes cryptographiques faibles, ont des vulnérabilités connues qui permettent leur clonage et des attaques par rejeu[16]. Il convient donc de s'orienter vers des produits fiables, récents, et dont le niveau de sécurité est satisfaisant. La certification de la puce aux critères communs EAL 4+ est un gage de sécurité.

Il est nécessaire de bien se renseigner lors de l'achat des badges et lors de l'installation du système pour s'assurer que les fonctionnalités d'authentification sont mises en place (certains installateurs maîtrisent mal ces technologies). A ce titre, les utilisateurs de systèmes de contrôle d'accès sont invités à s'inspirer des clauses proposées au chapitre 5. Ils peuvent également se tourner vers leurs organisations professionnelles, vers le CNPP et vers l'ANSSI afin de promouvoir la mise en place d'un schéma de certification des intégrateurs, des installateurs et des mainteneurs de ce type de systèmes.

4.1.2 Têtes de lecture : protection des éléments chiffrés.

>> Les parties du système situées hors de la zone de sécurité délimitée par le contrôle des accès, dont les têtes de lecture font partie, ne doivent pas être source de vulnérabilités.

Dans le cas des architectures où les têtes de lectures renferment des éléments secrets, celles-ci doivent comporter des mécanismes de protection tels que l'effacement des clés et éventuellement le déclenchement d'une alarme en cas d'arrachement. Malheureusement ces dispositifs ne sont pas totalement sûrs : pour la plupart des produits proposant ces fonctionnalités, il demeure possible d'accéder à l'intérieur de la tête avec un espacement très réduit (moins de 5mm) sans les déclencher. Bien que ce mode d'attaque soit d'un niveau déjà avancé, il confirme la nécessité d'exercer une surveillance des points d'accès permettant de déceler toute activité suspecte sur les lecteurs.

Ces architectures requièrent également une méthode de mise à la clé sécurisée.

En outre, du fait du nombre restreint de fabricants de lecteurs et de badges, certains modèles sont facilement reconnaissables et peuvent révéler la technologie employée. Il est donc conseillé d'utiliser

[15] *Radio Frequency Identification.*
[16] Attaque dans laquelle une transmission est frauduleusement répétée par une tierce partie interceptant les paquets sur la ligne.

des lecteurs à façades standards ou anonymes (soit, totalement dépourvus d'un quelconque sigle de société ou de marque).

Enfin, il est nécessaire de connaître les personnes habilitées à effectuer le paramétrage et les opérations d'entretien des lecteurs (mise à la clé, maintenance, etc.) et d'assurer un suivi des opérations requérant ces accès.

4.1.3 Unités de traitement local : accès physique réservé, Secure Access Module et redondance.

L'unité de traitement local (UTL) se présente généralement sous la forme d'une carte à circuits imprimés, que l'on peut considérer comme un automate, et qui gère un groupe de têtes de lecture, généralement chacune associée à un ouvrant.

C'est un élément particulièrement sensible du système de contrôle d'accès : il détient un cache de la base des droits d'accès, ainsi que d'autres informations telles que les derniers journaux d'événements. Dans la plupart des architectures, l'UTL détient aussi les éléments secrets cryptographiques permettant l'identification/l'authentification et la sécurisation de la communication avec le badge ou les têtes de lecture. Enfin l'UTL contient les relais qui commandent l'ouverture des ouvrants.

>> Les UTL doivent donc impérativement être situées à l'intérieur de la zone physique pour laquelle elles commandent l'accès et ne doivent pas être accessibles facilement (idéalement, elles doivent être à l'abri de tout accès frauduleux, dans un local technique ou tout autre type d'emplacement sécurisé).

>> Les UTL sont parfois maintenues par des personnes tierces non habilitées à accéder aux clés cryptographiques. Ce problème ne se pose pas dans le cas de l'architecture présentée en annexe 2 (la plus répandue actuellement), mais le risque existe dans le cas de l'architecture n°1 qui reste pourtant la seule recommandable. Une solution consiste à utiliser des modules sécurisés de type « *Secure Access Module*[17] » (SAM) afin d'isoler et de protéger les éléments secrets au sein de l'UTL. *(voir également en 4.2)*

>> Dans le cadre de la maintenance globale du système, la batterie de l'alimentation de secours de l'UTL doit être régulièrement vérifiée. Cette alimentation de secours et la réplication de la base des droits d'accès dans chaque UTL sont le gage d'une grande résilience du système.

>> Comme pour la maintenance des têtes de lecture, il est impératif de disposer de la liste des personnes autorisées à accéder physiquement aux UTL et d'assurer également la surveillance de ces opérations.

4.1.4 Liaisons filaires : dans le périmètre de sécurité.

Autant que possible, les liaisons filaires doivent être situées dans la zone de sécurité délimitée par le contrôle des accès, et non pas à l'extérieur de cette zone.

4.1.5 Réseau fédérateur : chiffrer les communications, protéger l'intégrité.

Concernant les liaisons entre les UTL et le serveur de gestion du système de contrôle des accès (dites liaisons filaires du réseau fédérateur), la problématique est sensiblement la même. Que l'on soit dans un schéma « mono-site », ou « multi-sites » » avec des liaisons filaires extérieures et éventuellement l'utilisation de passerelles IP (par exemple un serveur de gestion centralisé pilotant des sites éloignés connectés par VPN au site principal), le chiffrement de la communication est indispensable, à moins que les liaisons ne soient protégées en intégrité (passages de câbles sous surveillance[18] ou trop difficile d'accès).

L'illustration ci-dessous présente une configuration.

[17] Dispositif généralement constitué d'une carte à puce au format d'une carte SIM, qui se charge de certains calculs cryptographiques en lieu et place du système sur laquelle on la connecte. Ce dispositif améliore la sécurité des clefs cryptographiques en les isolant. Il peut être utilisé par exemple pour effectuer des dérivations de clef en assurant la sécurité de la clef maîtresse, qu'il protège.

[18] Notion de circuit approuvé.

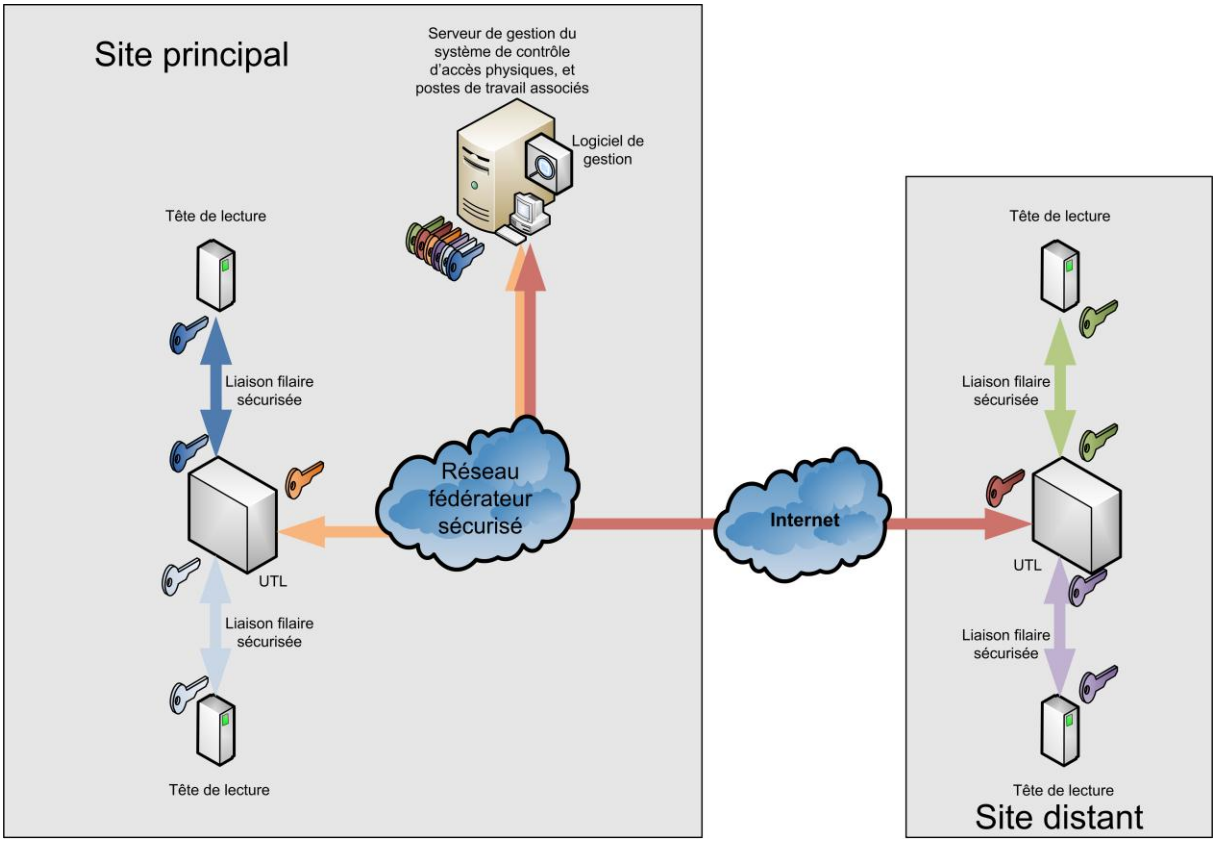


Figure 4 : exemple d'un système de contrôle d'accès sans contact

4.1.6 Serveur de gestion du système et postes de travail : un SI à part entière

Le serveur de gestion du système est aussi appelé Unité de Traitement de Supervision (UTS) ou Gestion des Accès Contrôlés (GAC).

>> Le système de contrôle d'accès est un système d'informations (SI) à part entière. Il doit donc être sécurisé comme tout SI et ce, d'autant plus qu'il traite d'informations personnelles sensibles.

Il faut que les configurations du serveur de gestion du système de contrôle des accès, ainsi que des postes de travail relatifs au contrôle des accès, soient sécurisées par l'application des mesures habituelles de sécurité des SI (pare-feu, application régulière des correctifs de sécurité, antivirus, bonne gestion des comptes utilisateurs, authentification forte, etc.)[19].

Le respect d'une hygiène informatique stricte est d'autant plus crucial lorsque le système de contrôle d'accès est connecté à d'autres systèmes - tel un circuit de vidéo surveillance, surtout si ce dernier est constitué de caméras IP ou un système de gestion du personnel avec interconnexion au réseau local (voir aussi Chapitre 6.1.1 : *Interconnexion avec un système de gestion des ressources humaines* et Chapitre 6.1.4 : Interconnexion avec les systèmes de surveillance vidéo).

Ces machines doivent être physiquement protégées de la même manière que les UTL.

[19] L'ANSSI publie un de nombreuses recommandations sur son site : http://www.ssi.gouv.fr/bonnes-pratiques

4.1.7 Logiciel de gestion du système : le point névralgique des systèmes de gestion d'accès physiques par technologie sans contact.

Le logiciel installé sur le serveur de gestion a pour rôle de communiquer d'un point de vue logique avec les UTL[20]. Ce logiciel enferme toute l'intelligence applicative, les autres éléments, sous sa commande, n'étant généralement que des automates peu évolués. Il doit donc être doté de toutes les fonctionnalités nécessaires afin de piloter efficacement les UTL et en particulier :

- la centralisation des journaux d'événements des UTL, pour archivage sécurisé et consultation en temps réel ;
- la remontée des événements au gestionnaire, que ce soit sous la forme d'alertes lors de tentatives d'accès non autorisées ou de défectuosité d'un équipement, ou régulières sous la forme de rapports journaliers par exemple ;
- la gestion des badges, des droits, des groupes, des dates d'expiration, etc. ;
- la maintenance en temps réel de la base de données centrale contenant toutes ces informations ;
- la sauvegarde régulière de la base de données ;
- le pilotage en temps réel de l'ensemble des UTL, en leur transmettant la base de données nécessaire à leur traitement des demandes d'accès ;
- l'authentification pour contrôler l'accès au logiciel, et éventuellement la gestion de droits associée.

4.2 Principes cryptographiques mis en contexte

Acquérir des badges supportant l'authentification et disposant de mécanismes cryptographiques ne suffit pas. Il faut activer correctement ces mécanismes lors de l'installation par l'intégrateur, faute de quoi, les badges ne seront utilisés qu'en identification, et pourront donc être clonés.

Les mécanismes cryptographiques devraient respecter les règles fixées par l'ANSSI précisées dans le document public : « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » qui constitue l'annexe B.1 du Référentiel Général de Sécurité (RGS) accessible sur le site de l'ANSSI[21]. D'autres référentiels existent, correspondant à des niveaux de sécurité supérieurs, qui peuvent être consultés en fonction de la sensibilité du lieu où est mis en place le système de contrôle des accès.

Les mécanismes d'authentification cryptographique doivent être documentés. Il ne doit pas y avoir d'attaques connues permettant de cloner la carte, ou de rejouer une transaction.

La taille des clés utilisées devrait également être conforme au Référentiel de l'ANSSI.

Le mécanisme d'authentification peut employer trois types de clés :

- une clé symétrique unique

  La même clé secrète est employée par toutes les cartes et par tous les systèmes de contrôle. Cette distribution à grande échelle représente un risque pour cette clé, qui pourrait être compromise par l'attaque matérielle d'une carte, ou du système de contrôle.

- des clés symétriques dérivées d'une clé maîtresse

  Chaque carte contient une clé différente, qui est dérivée par un mécanisme cryptographique à partir d'une clé maîtresse et d'un identifiant unique (UID) propre à chaque carte. L'UID est également contenu dans la carte.

[20] Le logiciel et le serveur de gestion du système peuvent être intégrés dans un « boitier logiciel » (*appliance*).
[21] Voir sur le site Internet de l'ANSSI : www.ssi.gouv.fr/rgs

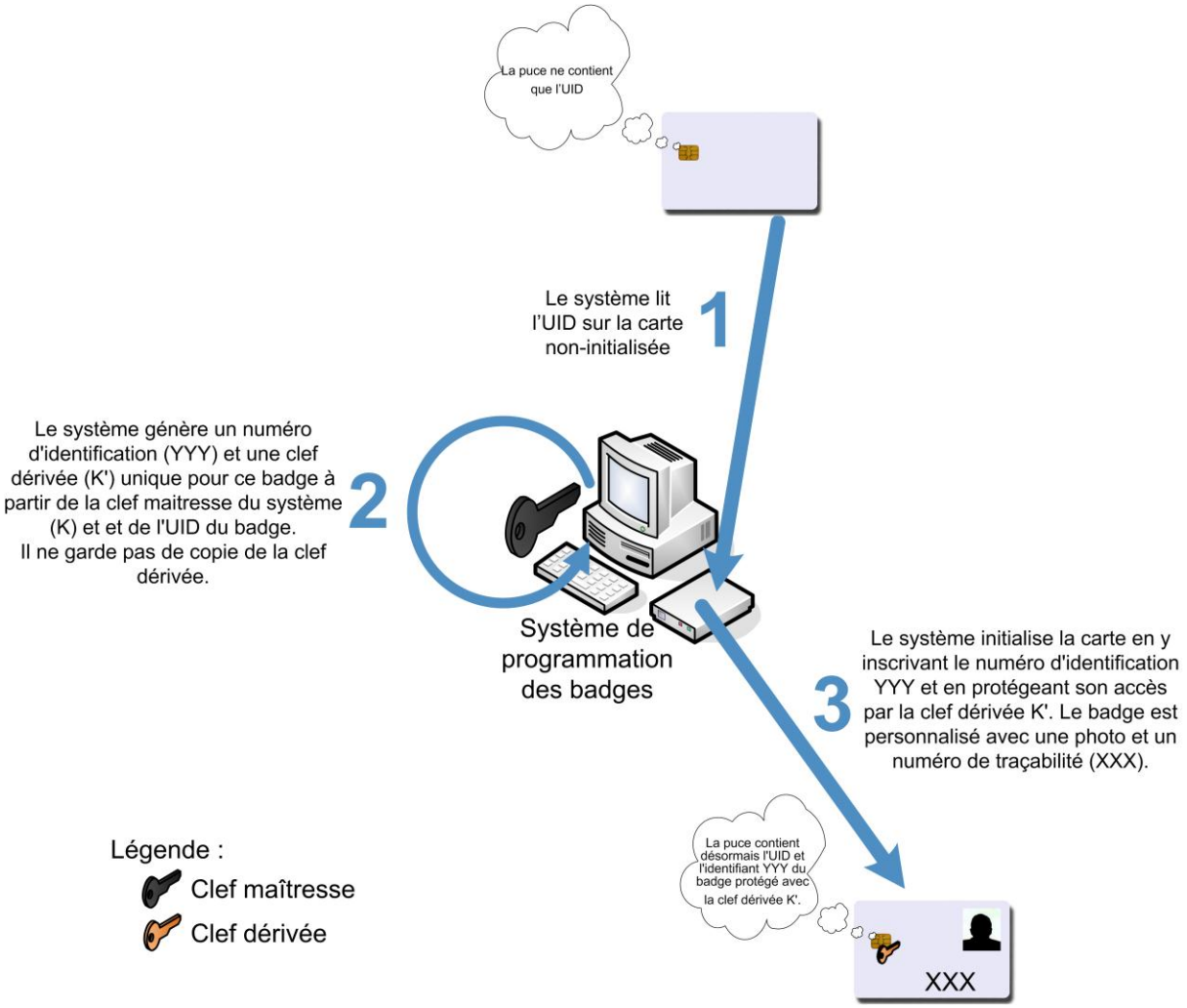


Figure 5 : Processus d'initialisation des badges à clef symétrique dérivée

Lors du contrôle, le système demande l'identifiant unique de la carte, puis, à partir de la clé maîtresse et de l'UID du badge, regénère la même clef dérivée, ce qui permet d'authentifier cette carte.

L'avantage de cette approche est que l'attaque matérielle d'une carte ne permet que de la cloner. Elle ne permet pas d'en forger une différente, car la clé maîtresse n'est pas présente au sein de la carte.

En revanche, la clé maîtresse doit être employée par le système de contrôle lors de chaque vérification. Afin de mieux protéger celle-ci, il est recommandé d'utiliser le module appelé *Secure Access Module* (SAM), carte à puce qui renferme la clé maîtresse, et qui produit elle-même les clés dérivées pour le système de contrôle. Ce dernier ne manipule ainsi jamais la clé maîtresse qui reste protégée dans le SAM.

- des clés asymétriques

  Chaque élément du système possède sa propre clef privée, qui permet le déchiffrement de messages chiffrés avec la clef publique. Plus flexible, cette solution permet de mieux protéger les éléments les plus sensibles (les clés privées) en n'utilisant que des clés publiques et des certificats lors du contrôle.

  Il s'agit de la solution la moins répandue car elle nécessite des cartes sans contact puissantes pour que le délai de vérification ne soit pas prohibitif. Elle est néanmoins la plus sécurisée car en cas de compromission, de perte ou de vol, seule la clef concernée devra être révoquée et changée.

La création et la gestion de toutes les clés cryptographiques employées dans le système de contrôle des accès physiques sont des opérations essentielles pour la sécurité du système. Lors de ces opérations, il est essentiel d'assurer la protection des clés cryptographiques car elles sont le facteur principal de la sécurité du système.

>> Pour cela, il convient de suivre les recommandations du référentiel de l'ANSSI, et de faire réaliser ces opérations sous le contrôle du gestionnaire du ou des sites.

Une attention particulière doit être apportée à la méthode de mise à la clé du système de contrôle des accès, notamment dans le cas où les têtes de lecture renferment des clés.

>> Il ne doit pas être possible pour une personne extérieure (y compris le fournisseur du matériel) de changer les clés d'authentification sans que cela ne soit détecté.

En cas de compromission d'une clé, il est souhaitable que le responsable du système de contrôle d'accès puisse changer les clés cryptographiques qu'il emploie, sans entraîner de surcoûts (rachat de cartes) ou de perturbations dans son service aux usagers, ni introduire de nouvelles failles de sécurité.

Si plusieurs zones sont de sensibilités différentes, ou sont sous la responsabilité de différents organismes indépendants, il est souhaitable que des clés cryptographiques différentes soient utilisées pour chaque niveau (ou organisme).

Cela permet de s'assurer que la compromission de la clé d'une zone peu protégée n'entraîne pas la compromission d'une zone plus protégée.

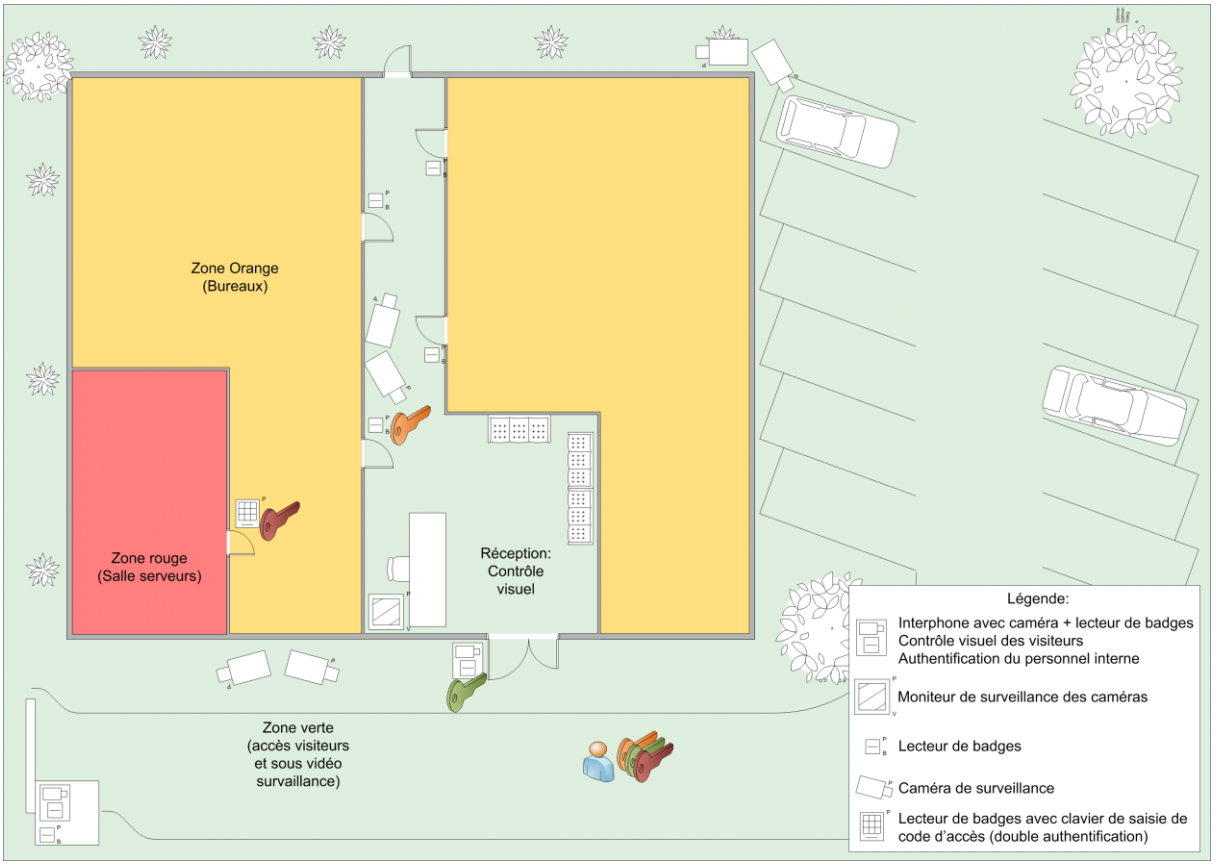


Figure 6 : différentiation des clefs utilisées selon la sensibilité des zones

En pratique, il s'avère souvent nécessaire d'employer d'autres clés cryptographiques dans le système de contrôle des accès, notamment :

- la ou les clés permettant d'écrire dans les cartes (écriture de champs, écriture de clés, formatage).
- la ou les clés permettant de configurer et d'injecter les clés dans le système de contrôle (tête de lecture, UTL ou SAM).

Par leur usage, ces clés sont une information d'une grande sensibilité. Cependant, n'étant pas nécessaires lors du contrôle (où seule la clé d'authentification est utilisée), elles ne sont employées que lors de la création de badges et la configuration du système. Elles peuvent donc être plus facilement protégées et conservées de façon sécurisée (par exemple dans une enveloppe scellée mise dans un coffre-fort) au sein d'un des sites protégés.

4.3 Architectures

Le choix d'une architecture avec têtes de lecture passives (qui se contentent simplement de transférer les messages) permet de s'affranchir des problématiques de sécurité des liaisons filaires entre les têtes de lecture et les UTL, dans la mesure où le badge est sécurisé. Dans le cas contraire, les informations circulant dans les liaisons filaires extérieures doivent être protégées en confidentialité et en intégrité.

Il existe différents types d'architectures, faisant intervenir les trois éléments supports principaux : le badge, la tête de lecture, et l'unité de traitement local (UTL). Ces éléments interviennent à différents niveaux et avec des mécanismes de sécurité variables.

Quatre architectures sont présentées dans ce guide, par niveau de sécurité décroissant.

Les architectures 3 et 4 sont déconseillées.

4.3.1 Architecture n°1, hautement recommandée

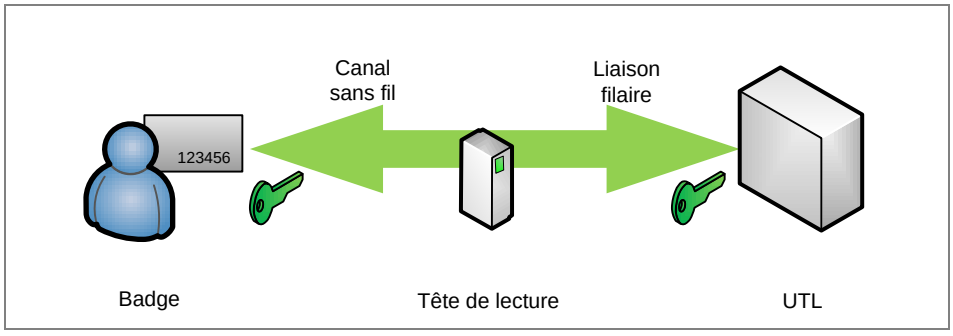


Figure 7 : Architecture n°1 : tête de lecture transparente, authentification de bout en bout

Le badge, sécurisé[22], s'identifie et s'authentifie directement à l'UTL par l'intermédiaire de la tête de lecture qui transmet les messages sans les modifier, et ne participe pas au protocole cryptographique (tête de lecture dite « transparente »).

Avantages :

- le badge, sécurisé, ne peut pas être cloné ;
- aucune information ne circule en clair, que ce soit sur le canal sans fil ou sur la liaison filaire ;
- la tête de lecture ne contient aucun élément secret : il n'y donc aucun impact en cas d'exploitation d'une vulnérabilité de cette dernière.

Inconvénient :

- l'UTL doit avoir la capacité d'effectuer le protocole d'authentification.

>> Cette architecture est hautement recommandée, bien qu'elle reporte le risque d'exploitation d'une vulnérabilité de la tête de lecture sur l'UTL. Les mesures de protection concernant l'UTL devront donc requérir une attention toute particulière, notamment pour la protection des clefs cryptographiques (voir Chapitre 4.1.3 : « Unités de traitement local »).

[22] Idéalement certifié Critères Communs au niveau EAL4+.

4.3.2 Architecture n°2, acceptable

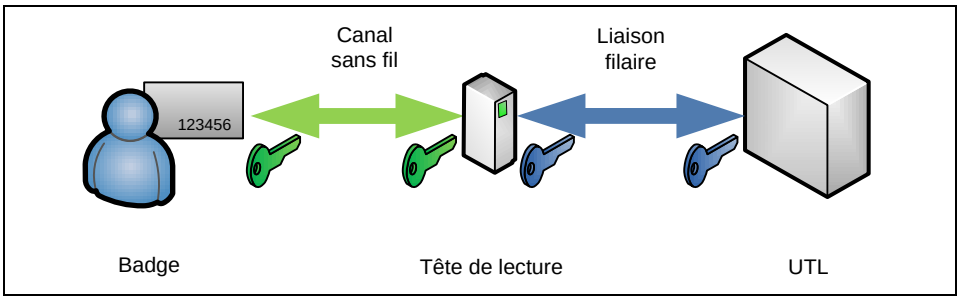


Figure 8 : Architecture n°2 : tête de lecture intelligente, double authentification en coupure

Le badge, sécurisé[23], s'identifie et s'authentifie à la tête de lecture. Cette dernière a également une liaison sécurisée (avec authentification et garantie de l'intégrité) avec l'UTL. Elle envoie l'identité récoltée à l'UTL.

Avantages :

- le badge, sécurisé, ne peut pas être cloné ;
- la liaison filaire est protégée.

Inconvénients :

- 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 ;
- le badge est authentifié indirectement par l'UTL. La tête de lecture est un intermédiaire dont le bon fonctionnement est crucial pour la sécurité du système.

>> Cette architecture est acceptable si la tête de lecture a fait l'objet d'une étude de sécurité approfondie.

4.3.3 Architecture n°3, déconseillée

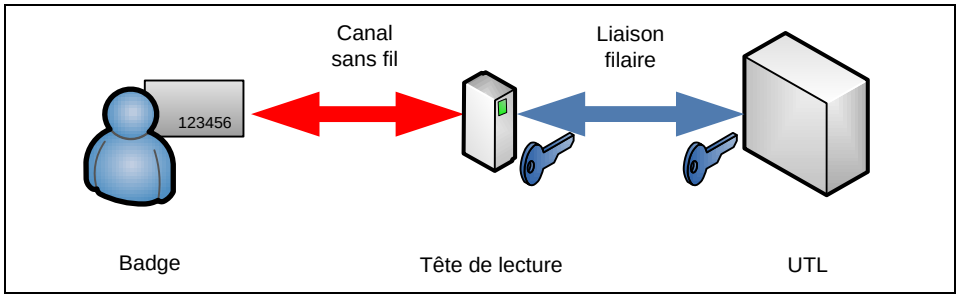


Figure 9 : Architecture n°3 : Badge non sécurisé, avec chiffrement filaire seulement

Le badge, non sécurisé, s'identifie directement auprès de l'UTL. La liaison filaire entre la tête de lecture et l'UTL est protégée.

Avantage :

- la liaison filaire est protégée.

Inconvénients :

- le badge peut être cloné, y compris hors du site, ce qui rend sans intérêt la protection filaire. Il ne sert que d'identification.
- les éléments secrets permettant la protection de la liaison filaire se situent dans la tête de lecture, qui se trouve hors de la zone de sécurité.

Cette architecture est **déconseillée**.

[23] Idéalement certifié Critères Communs au niveau EAL4+.

4.3.4 Architecture n°4, déconseillée

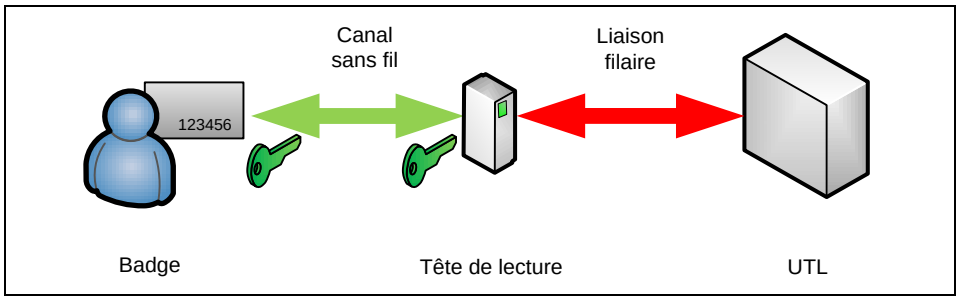


Figure 10 : Architecture n°4 : Badge sécurisé, avec liaison filaire non chiffrée

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

Avantage :

- le badge, sécurisé, ne peut pas être cloné.

Inconvénients :

- la liaison filaire n'est pas protégée : un attaquant peut contourner l'authentification s'il se branche physiquement sur la liaison filaire.
- la clé secrète d'authentification est stockée dans la tête de lecture, qui se trouve hors de la zone de sécurité.

Cette architecture est **déconseillée** si le site ne fait pas l'objet d'une surveillance physique renforcée.

En revanche, il est possible de migrer de cette architecture vers l'architecture 1 si la tête de lecture est capable de passer en mode transparent, et si les UTL sont changées.

5 Spécifications

Lors de la phase de préparation du cahier des charges en vue de la passation d'un marché pour l'acquisition et l'installation d'un système de contrôle d'accès sans-contact, il est recommandé de rendre ce guide applicable et d'inclure les clauses présentées en Annexe 4 - Spécifications détaillées en vue d'une passation de marché.

Ces spécifications sont présentées selon 13 grands thèmes correspondants aux différents éléments du système ou à son installation et sa maintenance :

- Technologie utilisée ;
- Badges ;
- Têtes de lecture ;
- UTL ;
- Réseaux et communications ;
- Performances ;
- Résilience ;
- Horodatage et contrôle des accès ;
- Gestion des alarmes et événements ;
- Stockage et archivage ;
- Biométrie ;
- Installation ;
- Maintenance.

Note : les exigences indiquées sont complémentaires :

- Pour atteindre un niveau de sécurité de niveau L1, il faut appliquer toutes les exigences du niveau L1.
- Pour atteindre un niveau de sécurité de niveau L2, il faut appliquer toutes les exigences du niveau L1 et toutes celles du niveau L2.
- Pour atteindre un niveau de sécurité de niveau L3, il faut appliquer toutes les exigences du niveau L1, du niveau L2 et toutes celles du niveau L3.

Voir également :
Tableau 2 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques (4.1.1)

6 Installation du système

6.1 Interconnexions avec d'autres systèmes

Les systèmes de contrôle d'accès ne sont pas autonomes et doivent satisfaire des contraintes supplémentaires d'interconnexion, ce qui a, bien entendu, des impacts en termes de sécurité.

6.1.1 Interconnexion avec un système de gestion des ressources humaines

Cette interconnexion est tolérée par la norme simplifiée n° 42 de la CNIL. Elle peut en effet contribuer à une mise à jour plus efficace des droits d'accès si les deux applications ont été prévues dans ce sens (et si le système de gestion des ressources humaines (RH) est bien mis à jour en « temps réel »).

Elle s'avère pour l'instant plus pertinente pour une révocation de droits que pour une attribution. Néanmoins, il faut veiller à ce que puissent être gérés les cas particuliers (comme par exemple une personne rappelée d'urgence). Par ailleurs, l'ensemble des porteurs de badges peut ne pas coïncider avec l'ensemble des personnes recensées dans le système RH.

Une telle interconnexion implique souvent un lien entre le système de gestion des accès avec le réseau informatique local. Il convient alors de prendre toutes les mesures nécessaires pour garantir que l'accès au système de gestion du contrôle des accès physiques ne soit pas possible depuis le réseau local.

Pour les raisons de sécurité propres au système de contrôle des accès, il est préférable d'éviter une telle interconnexion entre réseaux informatiques et de privilégier des processus organisationnels RH d'arrivée et de départ faisant intervenir le gestionnaire des accès physiques le plus tôt possible.

6.1.2 Interconnexion avec le système de contrôle du temps de travail

La norme simplifiée n° 42 de la CNIL autorise que ces deux fonctionnalités soient « associées ». Néanmoins, en vue d'une déclaration à la CNIL, il est préférable que l'ensemble soit nativement pensé comme un projet global.

A l'usage, et compte tenu de la sensibilité du sujet, il semble préférable de disposer d'un système de pointeuse à proximité du contrôle d'accès qui pourra utiliser la même carte. Le système est alors susceptible d'être mieux accepté par les usagers. Cette solution permet par ailleurs d'éviter de nombreux cas particuliers problématiques (cas des réunions à l'extérieur par exemple).

Une telle interconnexion est **déconseillée**.

6.1.3 Interconnexion avec les systèmes d'alertes en cas de catastrophe

L'interconnexion avec les systèmes d'alertes (c'est-à-dire d'incendie uniquement dans la plupart des cas) est une obligation réglementaire (Cf. Annexe 4).

6.1.4 Interconnexion avec les systèmes de surveillance vidéo

L'interconnexion au système de vidéo surveillance est acceptable si la sécurisation de ce dernier suit les mêmes principes que la sécurisation du système de contrôle des accès. Dans le cas d'une vidéo surveillance sur IP, plusieurs cas se présentent :

- Vidéo surveillance sur câblage IP dédié.

  Si la sécurité physique du câblage est assurée, l'interconnexion ne devrait pas poser de problèmes de sécurité. Il convient tout de même de vérifier attentivement les opérations de maintenance du système de vidéo surveillance, qui donne inévitablement accès à celui de contrôle des accès.

- Vidéo surveillance sur câblage IP du réseau informatique local.

  Dans ce cas précis, des mesures de cloisonnement doivent être mises en place afin que l'accès au système de gestion du contrôle des accès physiques ne soit pas possible depuis le réseau informatique local. Il est préférable, par sécurité pour le système de contrôle des accès, d'éviter une telle interconnexion.

6.1.5 Contraintes règlementaires

Certaines interconnexions peuvent être sujettes à des réglementations particulières. Un aperçu des principales règlementations est donné en Annexe 4.

6.1.6 Certification des intervenants

La complexité des systèmes, que le lecteur aura perçue tout au long de ce guide, nécessite qu'ils soient installés et maintenus par des personnes de confiance parfaitement formées. Pour pouvoir garantir la compétence de ces personnes, il semble utile de mettre en place un schéma de certification des personnes par des organismes habilités par le CNPP ou l'ANSSI.

Lors de l'écriture de ce guide, un tel schéma n'existe pas encore et seules des discussions informelles ont eu lieu sur ce sujet. Les utilisateurs, fournisseurs, intégrateurs et mainteneurs de systèmes de contrôle d'accès intéressés par la mise en place d'un tel schéma sont invités à se rapprocher de leurs organismes professionnels ainsi que du CNPP et de l'ANSSI pour en promouvoir l'idée.

7 Exploitation du système

7.1 Gestion des droits et des badges d'accès

Les droits d'accès doivent être définis pour chaque catégorie de personnes à même de s'introduire dans le ou les sites sous contrôle. Il est donc préférable de configurer les droits par groupes d'utilisateurs puis d'ajouter des accès personnalisés. Les procédures de définition des groupes et des droits individuels dans l'organisme doivent être formalisées dans ce sens, et être généralement validés par les chefs d'établissements ou autres personnes responsables.

7.1.1 Accès génériques

Les demandes de badges doivent être intégrées au processus de gestion des ressources humaines, lors de l'arrivée des salariés. Les droits spécifiques (par exemple : accès à la salle serveurs) éventuellement demandés devraient être validés par les chefs d'établissements ou autres personnes responsables.

La création (programmation) et la remise des badges doivent se faire selon des procédures définies, avec une remise de badge en face à face. Dans le cas d'une gestion locale du système de contrôle des accès, la création et la remise du badge doivent être effectuées sous le contrôle du gestionnaire du système. Dans le cas d'une gestion centralisée du contrôle des accès, la création et la personnalisation des badges doivent se faire selon un processus connu du gestionnaire du système.

Lorsque la situation le permet (recrutement d'un stagiaire, contrat à durée déterminée, fin de mission anticipée, etc.), une date de fin de validité du badge doit être programmée.

La restitution des badges doit également être intégrée aux processus de gestion des ressources humaines, lors du départ des salariés, afin que les droits soient révoqués au plus tôt.

L'historique des accès doit être consultable. Une vérification régulière des accès utilisateurs doit être effectuée.

7.1.2 Accès particuliers

Certains profils particuliers d'usagers occasionnels (personnel de maintenance, visiteurs, etc.) doivent être traités différemment des salariés tout en maintenant les mêmes exigences de sécurité (la sécurité générale du système repose sur la prise en compte du maillon le plus faible). En effet, les badges des personnels tiers sont plus facilement oubliés ou perdus, et parfois ne sont tout simplement pas restitués. S'ils sont moins sécurisés, ils offrent plus facilement à une personne mal intentionnée la possibilité de s'introduire dans l'enceinte sous contrôle.

- Les visiteurs

  En l'absence de mécanisme de dérivation de la clé maîtresse d'authentification [Cf. 4.2 Principes cryptographiques], et s'il existe des zones inaccessibles aux visiteurs ou dans le cas d'un organisme multi-sites, il est conseillé d'utiliser des clés de chiffrement différentes pour ces badges. De même, il est recommandé de limiter leur durée de validité.

  Il convient également de définir les procédures d'obtention d'un badge pour un visiteur ainsi que les modalités d'entrée dans les locaux de ce dernier. Les procédures peuvent être différentes selon le statut du personnel qui accueille le visiteur (un stagiaire peut ne pas être autorisé à faire entrer une personne extérieure, contrairement à un salarié). Dans tous les cas, les procédures doivent être documentées.

  Selon le niveau de sécurité recherché, en particulier si l'on souhaite qu'un visiteur ne puisse pas se déplacer seul, le système pourra être configuré de façon à ce que l'accompagnateur et le visiteur doivent effectuer une lecture de leurs badges dans un temps restreint sur un même point d'accès (fonction d'escorte).

- Les usagers privilégiés, ayant des droits importants

  La possibilité d'accorder à des porteurs du badge des droits importants (accès complet, reprogrammation des lecteurs, etc.) est à étudier au cas par cas. Le nombre de ces porteurs doit être réduit au strict nécessaire car ils représentent une importante et réelle vulnérabilité du système.

Lorsque de tels porteurs de badge existent, il est très fortement recommandé que leur badge demeure à l'intérieur de l'enceinte chaque fois que cela est possible. Dans ce cas, le porteur pourrait se voir remettre un badge permettant, dans un premier temps, d'accéder uniquement à l'intérieur de l'enceinte puis dans un deuxième temps de se faire remettre le badge ayant des droits plus importants).

7.1.3 Oubli, perte ou vol de badge

L'oubli du badge permanent doit se traduire par la délivrance d'un badge de substitution d'une durée de validité limité (24 heures maximum). Parallèlement, cela devrait entraîner l'invalidation temporaire du badge oublié. Il convient de vérifier qu'une même personne ne demande pas systématiquement un badge de substitution, ce qui révèlerait une probable perte non déclarée du badge permanent.

En cas de perte ou vol de son badge, le personnel concerné doit le signaler sans délai afin de faire invalider son badge.

7.2 Surveillance des accès

7.2.1 Analyse des journaux d'événements

Les journaux d'événements, centralisés de manière exhaustive par le logiciel de gestion du système de contrôle des accès, doivent être consultables facilement par le gestionnaire du système.

Des vérifications régulières des accès devraient être effectuées afin de détecter toute erreur ou anomalie. Ceci consiste par exemple à générer et examiner :

- un rapport listant les badges qui n'ont pas été utilisés lors des dernières semaines (5 par exemple), permettant de s'assurer que les badges sont bien tous actifs, et d'identifier des badges qui auraient dû être désactivés mais qui ne le sont pas ;
- la liste complète des accès visiteurs de la semaine ;
- un rapport d'utilisation des badges privilégiés sur la semaine écoulée ;
- la liste des accès refusés de la semaine, afin de détecter des tentatives d'accès frauduleuses répétées ;
- la liste des accès en dehors des plages horaires normales de travail et en dehors des jours ouvrés durant la semaine écoulée ;
- etc.

Une surveillance régulière et sérieuse des accès et des différents rapports est primordiale pour assurer la sécurité du système de contrôle des accès, en détectant rapidement les anomalies et les tentatives d'accès frauduleuses. **L'usage d'un faux badge sera très difficilement détectable autrement**.

7.2.2 Définition d'alertes spécifiques

En parallèle de rapports réguliers sur les journaux d'événements, il est recommandé de configurer des alertes en temps réel qui pourront être rapidement prises en compte par le gestionnaire du système. Ces alertes, qui se devront d'être peu nombreuses, pourront être remontées par exemple par courriel ou par des messages textes envoyés sur des téléphones portables (SMS), de manière à être rapidement consultées.

Bien entendu cela implique soit une interconnexion avec le réseau local pour permettre l'utilisation de services de messagerie, soit un réseau dédié au système et connecté aux postes de travail de gestion du système de contrôle d'accès (c'est-à-dire les postes des gestionnaires du système). Cette interconnexion devra être étudiée conformément au paragraphe 3.9.

Ces alertes devraient être configurées pour tout événement d'un niveau de criticité important.
Par exemple :

- tentatives d'accès refusées et répétées (2 fois sur une même tête de lecture et sur une période donnée, ou 2 fois par le même badge par exemple) ;
- défectuosité d'un élément support (tête de lecture, UTL, alertes systèmes et applicatives du serveur de gestion du système d'accès) ;
- tentative unique d'accès refusée à une zone sensible ;
- porte restée ouverte plus d'un certain temps ;
  *(*liste *non exhaustive)*

7.3 Procédures d'exploitation particulières

7.3.1 En cas de fonctionnement dégradé

On définit le fonctionnement dégradé, dans le cadre de ce guide, comme le fonctionnement du système de manière partielle suite à un dysfonctionnement complet ou partiel des éléments qui le composent.

Plusieurs types d'événements peuvent se produire et entraîner un fonctionnement dégradé. Les événements peuvent aussi se cumuler. Il convient de faire face à chaque situation en définissant les bonnes procédures dès la mise en place du système.

- Panne d'une tête de lecture

  Le gestionnaire du système veillera à avoir des têtes de lecture en stock pour garantir leur remplacement le plus rapidement possible. Pendant la panne, et en fonction des exigences et de l'emplacement de la tête de lecture concernée, plusieurs solutions sont possibles :
  - laisser la porte ouverte, en acceptant le risque ;
  - contrôler les flux de personnes manuellement (par un agent de surveillance par exemple) ;
  - condamner la porte et obliger les personnes à emprunter un passage secondaire. Attention toutefois au fait que s'il s'agit d'une porte avec un système de contrôle d'accès en entrée et en sortie, sa condamnation peut aller à l'encontre de la réglementation sur la sécurité des personnes (Cf Annexe 4) ;
  - etc.

- Panne d'UTL

  La problématique est la même que pour une tête de lecture défaillante, à la différence que plusieurs têtes de lecture (celles contrôlées par l'UTL) seront non opérationnelles.

- Panne du serveur ou du logiciel de gestion du système d'accès

  Les UTL doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome. Pendant la panne, la création de badges et leur révocation n'est pas possible, ni la génération des rapports ou la consultation des événements. Cette situation est faiblement critique et devrait pouvoir être gérée facilement et sans gros impact. Il est toutefois nécessaire de mener, au plus vite, les opérations de reprise après incident, à partir des dernières sauvegardes.

- Coupure électrique

  Pendant la durée de la coupure, et si les conditions de sécurité des personnes le permettent, il est conseillé de vérifier manuellement le verrouillage de chaque porte sensible (portes extérieures des sites, et portes intérieures donnant accès à des zones sensibles) afin de s'assurer que les batteries ont bien pris le relai d'alimentation et assurent le verrouillage des portes.

  Lorsque la durée de la panne excède l'autonomie sur batterie des éléments supports du système de contrôle d'accès, la panne relève de l'incident grave (cf. : 7.3.2 En cas de crise ou d'incident grave).

  Il convient de porter une attention particulière aux portes qui pourraient rester verrouillées alors que la réglementation sur la sécurité des personnes en impose le déverrouillage.

7.3.2 En cas de crise ou d'incident grave

Une crise, ou un incident grave, dans le cadre de ce guide, sera tout incident rendant le système non opérationnel dans sa quasi-totalité.

Parmi ces incidents, on en distingue deux types :

- panne importante du système

  Dans ce cas précis, il faut faire face à une situation où le contrôle d'accès n'est plus opérationnel pour différentes raisons (dysfonctionnement logiciel avec corruption des bases de droits des UTL, panne électrique plus longue que l'autonomie des éléments support, etc.).

Dans une telle situation, deux choses sont à garder à l'esprit :

- des catastrophes pourraient se produire pendant ce laps de temps, la sécurité des personnes doit, bien entendu, continuer d'être assurée, c'est-à-dire que tout système de verrouillage de porte non alimenté en électricité doit tout de même permettre son ouverture en sortie ;
- le besoin d'entrer peut subsister en fonction de la situation. Les portes, dont le système de verrouillage condamne ces dernières lorsqu'il n'est plus alimenté, doivent pouvoir être ouvertes par un moyen mécanique (clef par exemple).

- attaques réussies menées par des personnes malveillantes, remettant en cause la fiabilité du système de contrôle

  Si la fiabilité du système de contrôle d'accès est remise en cause, par exemple par la diffusion sur internet d'une vulnérabilité et des moyens simples pour l'exploiter, l'intrusion de personnes malintentionnées est facilitée. Le système peut alors être considéré comme non opérationnel et l'entreprise devrait avoir prévu des procédures agents de sécurité qui effectuent des rondes dans les zones concernées.

7.3.3 En cas d'alerte incendie

La réglementation nationale impose que les issues et dégagements permettent une évacuation rapide en cas d'incendie[24]. Les accès ne sont alors plus contrôlés par le système mis en place. Selon les risques identifiés et les règles définies par l'organisme, il convient de déterminer comme le contrôle des accès peut être assuré dans un tel cas, par exemple grâce à des moyens humains ou vidéos.

Le responsable du site doit déterminer (et tester) à l'avance comment se passera le retour dans les locaux à l'issue d'une alerte :

- soit par l'ouverture complète des points d'accès (avec contrôle humain par exemple)
- soit via le fonctionnement normal du système (il faut alors pouvoir réinitialiser le système).

7.4 Maintenance

7.4.1 Certification des intervenants

Les prestataires de maintenance devraient être certifiés conformément au paragraphe 6.1.6.

7.4.2 Maintien en condition de sécurité

Les agents de l'ANSSI constatent quasi systématiquement lors de leurs interventions que les systèmes de contrôle d'accès ne sont pas maintenus en condition de sécurité. Une fois installés, l'important est qu'ils fonctionnent. Aussi seule une maintenance opérationnelle est effectuée. Ce comportement conduit les entreprises et les administrations à faire reposer la sécurité de leurs biens les plus précieux sur des systèmes fonctionnant avec des logiciels obsolètes, dont de nombreuses vulnérabilités sont connues et exploitées.

Cette situation est absolument anormale.

> ***>> Les contractants doivent exiger un maintien en condition de sécurité pour leurs systèmes de contrôle d'accès, au même titre que pour tout autre système d'information.***

A minima, les tiers en maintenance doivent :

- notifier la présence de vulnérabilités sur les produits dont ils ont la charge ;
- proposer la mise en place immédiate de mesures palliatives de ces vulnérabilités et un plan de déploiement rapide des correctifs dès lors qu'ils ont été publiés par l'éditeur des logiciels ;
- fournir un suivi des versions des logiciels et des correctifs déployés ainsi que l'écart entre ce qui est déployé et les versions et correctifs compatibles avec le système les plus récents. Ils devront détailler les risques encourus dès lors que les versions déployées ne sont pas les plus récentes ou que les correctifs de sécurité ne sont pas tous installés.

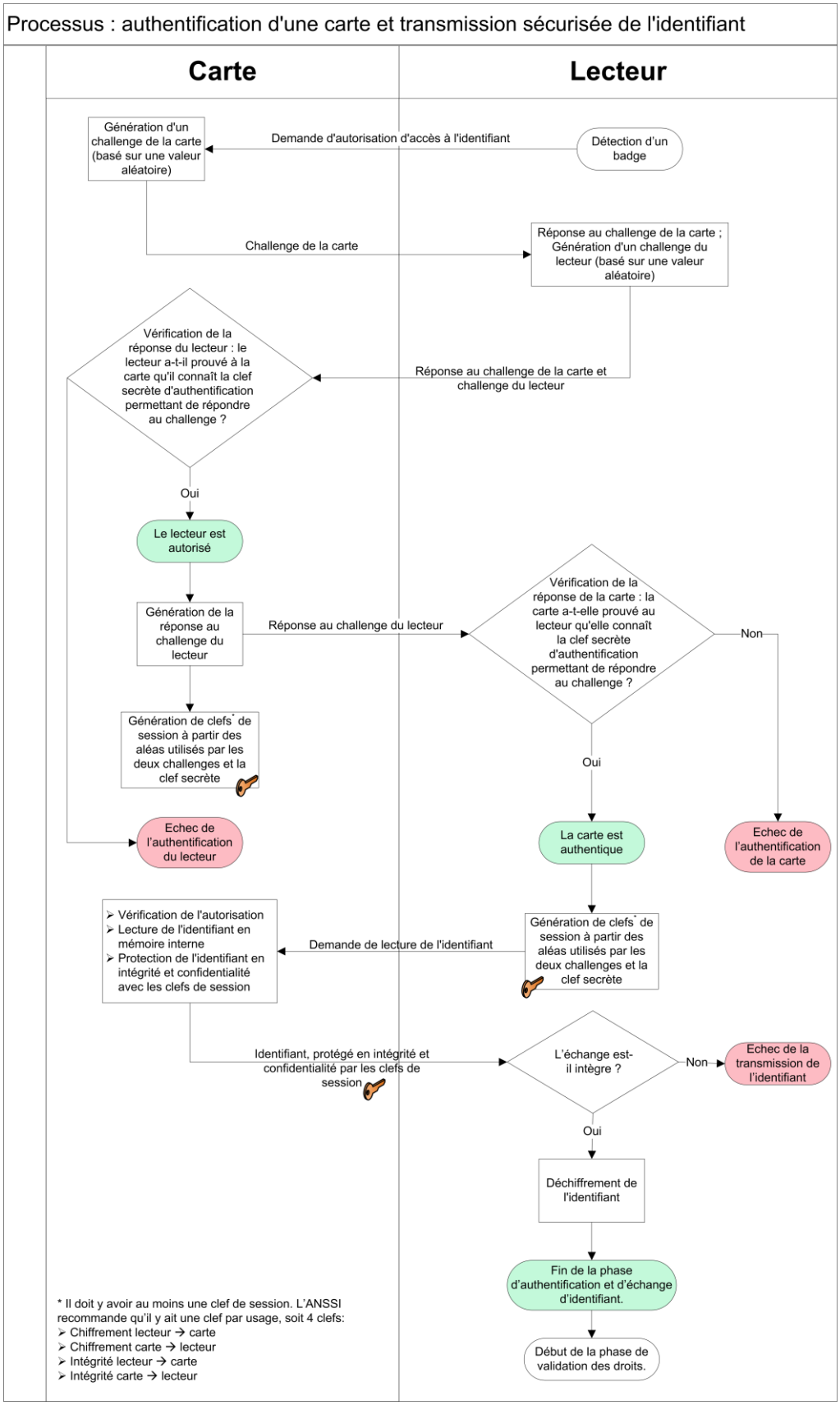
[24] Articles R4216-1 et suivants du Code du travail.

7.4.3 Télémaintenance

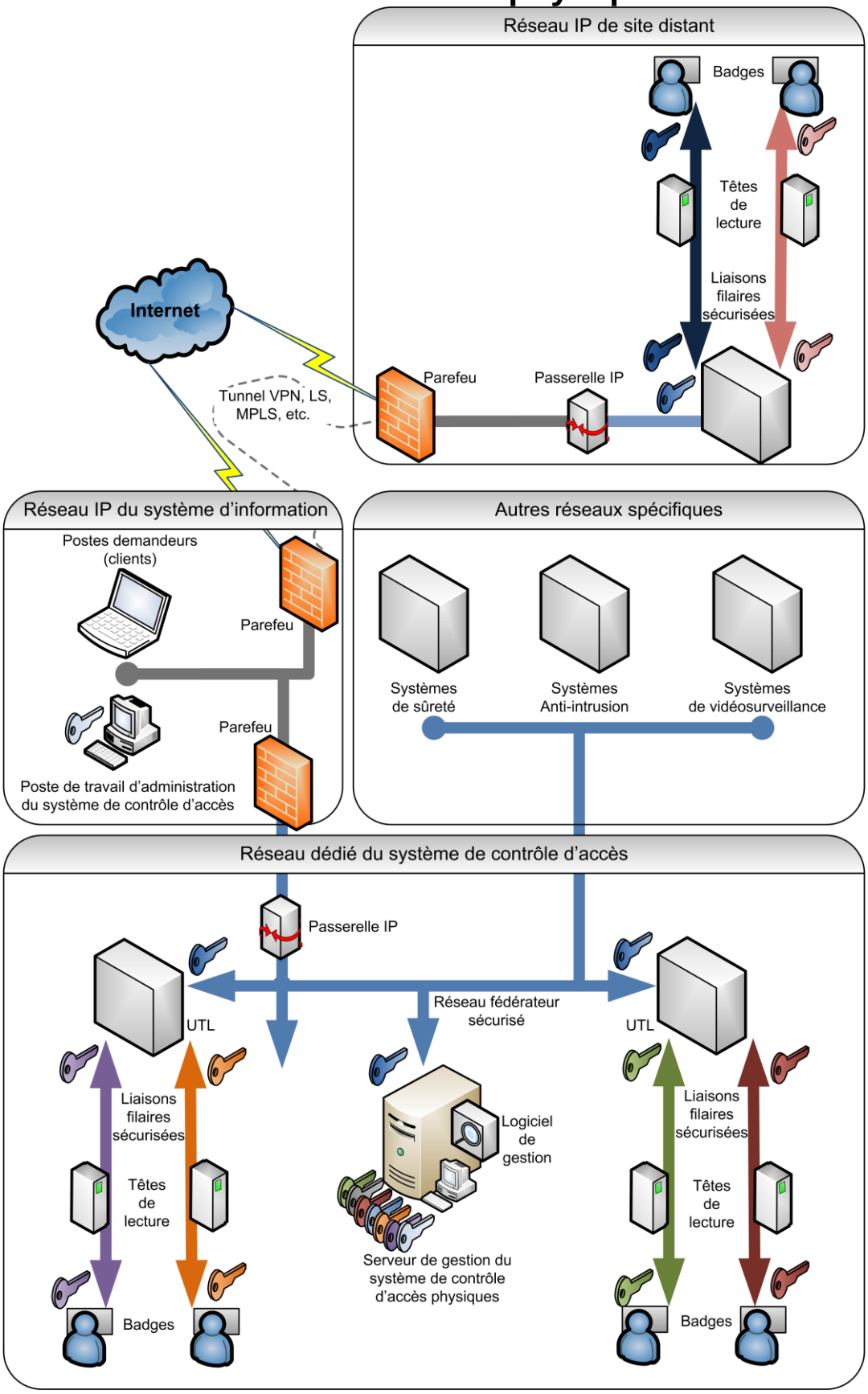
L'usage de la télémaintenance s'accompagne de risques parfois extrêmement élevés. Afin de les réduire, il est conseillé de suivre les recommandations du guide de l'ANSSI relatif à l'externalisation « Maîtriser les risques de l'infogérance »[25], notamment la partie 2.2 : Risques liés aux interventions à distance.

[25] http://www.ssi.gouv.fr/infogerance.

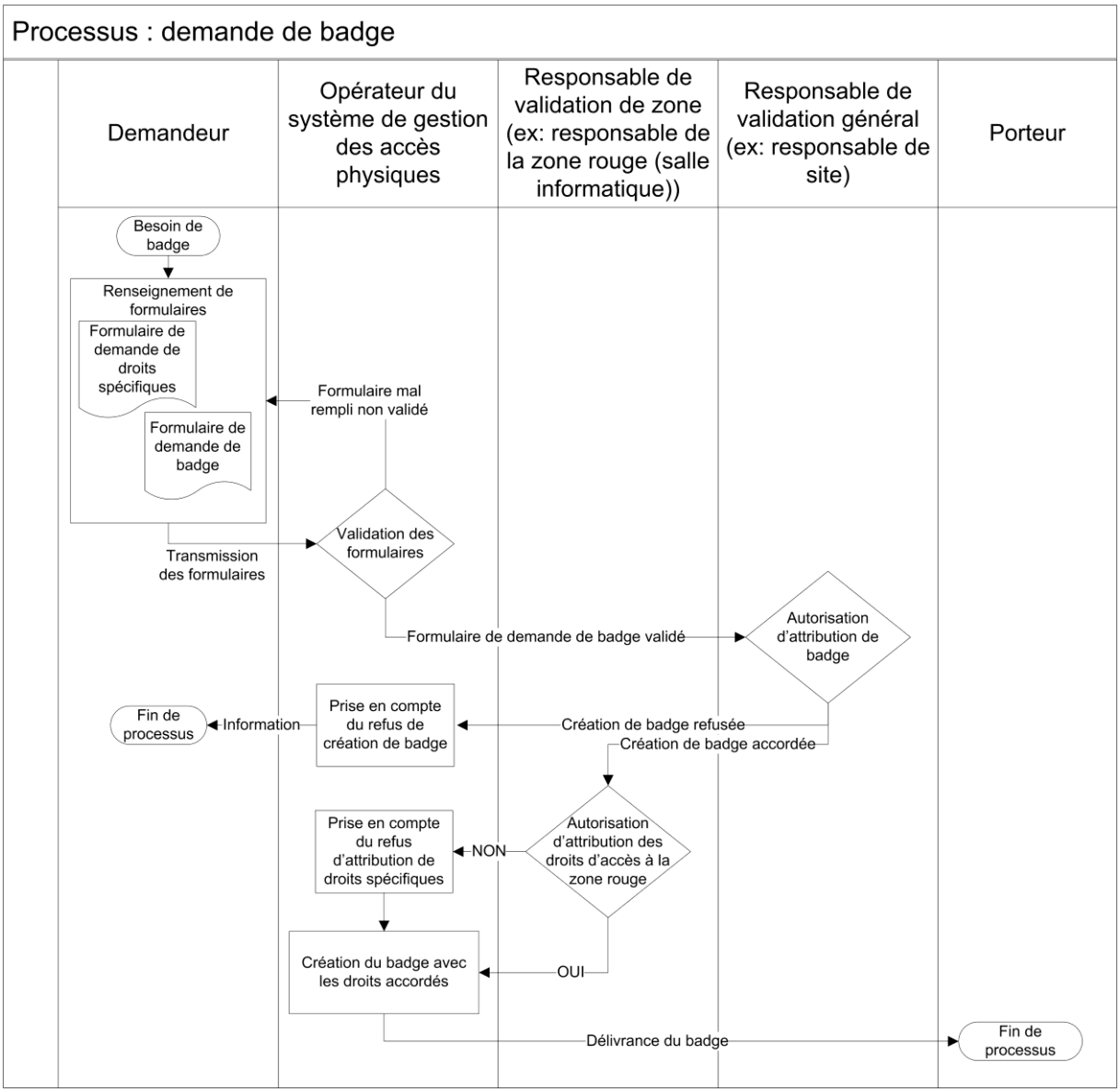
Annexe 1 Processus d'authentification d'une carte et de transmission sécurisée de l'identifiant



Annexe 2 Schéma général de l'architecture d'un système de contrôle des accès physiques multi-sites



Annexe 3 Exemple de processus organisationnel



Annexe 4 Spécifications détaillées en vue d'une passation de marché

A4.1 Technologie utilisée

L1 Une technologie conforme au niveau L1 du Tableau 2 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques, page 13 §4.1.1 - Badges : niveaux de sûreté, résistance aux attaques logiques. du guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques v1.0 de l'ANSSI sera mise en œuvre.

L2 Une technologie conforme au niveau L2 du Tableau 2 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques, page 13 §4.1.1 - Badges : niveaux de sûreté, résistance aux attaques logiques. du guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques v1.0 de l'ANSSI sera mise en œuvre.

L3 Une technologie conforme au niveau L3 du Tableau 2 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques, page 13 §4.1.1 - Badges : niveaux de sûreté, résistance aux attaques logiques. du guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques v1.0 de l'ANSSI sera mise en œuvre.

L3 Chaque support de l'identifiant utilisera une clé différente dérivée d'une clé maîtresse.

A4.2 Badges

L1 Les données relatives aux droits d'accès et les périodes de validité ne doivent pas être stockées dans le badge mais dans la base de données du système de contrôle d'accès.

L1 Le badge doit être garanti unique (aucun doublon avec un système existant dans la société ou dans une autre entreprise, et aucun doublon sur le même système).

L1 Le badge doit pouvoir être réaffecté à une autre personne sans perte de traçabilité.

L1 Aucune information relative au porteur du badge (excepté une photo de ce dernier) ou aux sites protégés ne doit être accessible sur celui-ci.

L1 Chaque badge doit se voir attribuer un numéro de traçabilité unique et visible sur le support. Ce numéro de traçabilité doit être différent du numéro d'identification du système.

L2 Le support de l'identifiant (badge, par exemple) doit être certifié selon les Critères Communs au niveau EAL4+.

L3 Pas d'exigence spécifique pour ce niveau.

A4.3 Têtes de lecture

L1 Les têtes de lecture doivent fonctionner avec une distance **maximale** de 5 cm entre le lecteur et le badge.

L1 Aucun droit d'accès ne doit être déporté dans la tête de lecture.

L1 Les têtes de lecture sont équipées d'un système de détection d'intrusion et d'arrachage.

L2 Les têtes de lecture doivent avoir démontré un excellent niveau de protection contre les fraudes. Elles devront avoir fait l'objet d'une certification de sécurité de premier niveau (CSPN)[26].

L2 Les têtes de lecture doivent comporter une signalisation visuelle d'accès autorisé et d'accès refusé, ainsi qu'une signalisation sonore en cas de porte maintenue ouverte.

L2 Les têtes de lecture ne doivent pouvoir être programmées que via les UTL, et en aucun cas au moyen d'une carte de maintenance simplement présentée à la tête de lecture pour la reprogrammer.

L3 Les têtes de lecture doivent pouvoir admettre un clavier d'authentification. Ce clavier devra être doté d'une fonction « accès sous contraintes ».

A4.4 UTL

L1 Les UTL et concentrateurs associés peuvent être associés en un seul et même équipement assurant les fonctions des deux.

L1 Les UTL analysent les droits du badge et délivrent l'ordre d'ouverture gâche ou actionneur.

L1 Pour leurs évènements et alarmes, les UTL assureront la datation.

[26] http://www.ssi.gouv.fr/cspn

L1 Les UTL transmettent les informations liées à la transaction, au serveur de gestion du système (UTS, GAC, ou autre équipement).

L1 Les UTL doivent émettre, vers le serveur de gestion du système, des informations sur les anomalies de fonctionnement qui leurs sont propres et sur les équipements qui leurs sont associés.

L1 Les UTL s'auto-surveilleront en générant des défauts internes. Ces alarmes seront datées et envoyées aux serveurs de gestion du système comme une alarme interne.

L1 Les UTL doivent réaliser des diagnostics fonctionnels sur les équipements qui lui sont associés.

L1 La sécurisation des UTL devra être cohérente avec la solution globale proposée.

L1 Les UTL sont installées à l'intérieur des zones qu'elles contrôlent.

L1 Les UTL sont équipées d'un système de détection d'intrusion et d'arrachage.

L1 Toutes les UTL pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.

L1 En cas de coupure de liaison avec le serveur de gestion du système, les UTL doivent pouvoir archiver temporairement un nombre d'alarmes ou d'événements compatible avec les exigences, puis assurer une mise à jour différée de l'archivage centralisé.

L1 En cas de coupure de liaison avec le serveur de gestion du système, les UTL doivent pouvoir gérer au minimum N badges.

L1 Les UTL possèderont une mémoire (contenant les instructions du traitement) type EPROM (*Erasable Programmable Read Only Memory*) ou RAM (*Random Access Memory*) sauvegardée par batterie (24 heures minimum).

L2 Les UTL doivent être capables de gérer « l'anti *pass-back* » des lecteurs qui lui sont associés.

L3 Pas d'exigence spécifique pour ce niveau.

A4.5 Réseaux et communications

L1 Les cheminements de câbles seront mis en place à l'intérieur des zones contrôlées.

L1 Les liaisons de communication entre les moyens physiques d'ouverture et l'unité de traitement local seront des liaisons dédiées au système de sécurité.

L1 Les liaisons filaires seront surveillées de manière à garantir qu'aucune tentative de fraude ne puisse être réalisée.

L1 La perte d'informations au niveau des liaisons devra être signalée et traitée comme une alarme.

L1 La fibre optique sera préférée pour les liaisons vers l'extérieur du bâtiment.

L2 La transmission des informations du système de contrôle d'accès se fait sur des VLANs dédiés à ce système.

L2 Les protocoles de communication utilisés (algorithmes de chiffrement inclus) devront être décrits, et particulièrement les principes de sécurisation et de vérification des échanges.

L2 La communication entre le badge, la tête de lecture et l'UTL sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS[27]).

L2 La communication entre l'UTL et le serveur de gestion du système sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS[28]).

L3 Les câbles servant pour la transmission des informations du système de contrôle d'accès sont des câbles dédiés à ce système.

L3 Les réseaux définis pour le système de contrôle d'accès seront totalement indépendants des réseaux du site autant pour les câbles que pour les équipements électroniques ou informatiques associés.

L3 S'ils venaient à faire l'objet de vulnérabilités publiées, permettant de compromettre leur efficacité, les protocoles et algorithmes utilisés devront pouvoir être remplacés par d'autres protocoles ou algorithmes ne faisant pas l'objet de vulnérabilités publiées et permettant de maintenir le niveau de sécurité des échanges.

[27] http://www.ssi.gouv.fr/rgs
[28] http://www.ssi.gouv.fr/rgs

A4.6 Performances

L1 Le temps de réponse entre la présentation d'un badge et l'ouverture doit être inférieur à 0,5 s.

L1 Le temps d'apparition d'une alarme sur une console d'exploitation (en service) doit être inférieur à 2 s.

L1 Le temps de transmission d'une information d'accès au serveur de gestion du système doit être inférieur à 2 s.

L2 Pas d'exigence spécifique pour ce niveau.

L3 Pas d'exigence spécifique pour ce niveau.

A4.7 Résilience

L1 Au niveau du système et des équipements, une alimentation de secours d'une autonomie de X heures minimum devra pallier à une perte de l'énergie principale (batterie /onduleur).

L1 Le constructeur s'engage à fournir du matériel de remplacement identique pendant Y ans.

L1 Tous les équipements seront dimensionnées en fonction des besoins en dégageant un potentiel de croissance de l'ordre de X% sur les entrées / sorties.

L2 Pas d'exigence spécifique pour ce niveau.

L3 Pas d'exigence spécifique pour ce niveau.

A4.8 Horodatage et contrôle des accès

L1 Toutes les données seront datées.

L1 La datation sera précise à la seconde près et le système garantira la synchronisation de tous les équipements entre eux.

L1 La mise à l'heure locale au niveau serveur de gestion système sera faite manuellement avec une possibilité de synchronisation externe par NTP (*Network Time Protocol*).

L1 Le passage en heure d'été/heure d'hiver sera automatique mais cette fonction pourra être désactivée.

L1 Le logiciel ne doit pas interdire le déverrouillage des accès par commandes manuelles (clé, coup de poing, etc.).

L1 Dans tous les cas, les demandes de commandes d'ouverture et fermeture doivent faire l'objet d'une information enregistrée par le système, en précisant l'origine de la commande (opérateur), à l'exception des dispositifs anti-panique du type « coup de poing », où seule l'information de début et fin doit être enregistrée.

L1 Le logiciel doit permettre d'autoriser l'accès ponctuellement à une ou plusieurs zones à un détenteur de badge en traçant l'ensemble des éléments de l'opération.

L1 Le système doit permettre d'effectuer des recherches sur la configuration opérationnelle.

L2 Le logiciel doit permettre de faire le comptage des personnels présents dans un local ou une zone contrôlée en entrée / sortie. Les détenteurs qui ne sont pas dans ces zones, doivent être identifiés dans une zone commune du site.

L2 Le logiciel doit pouvoir interdire l'accès à un local ou à une zone dès qu'un nombre de personnels programmé est dépassé.

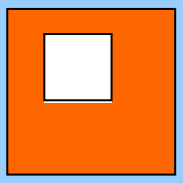
L2 Le logiciel doit posséder la fonction « anti *pass-back* » : le badge ne donne à nouveau l'entrée que lorsqu'il a été enregistré en sortie.

L2 Le logiciel doit posséder la fonction « escorte » : les badges visiteurs ne permettent l'accès qu'après le passage de la personne chargée de l'accompagner, et ce uniquement pendant un délai de X secondes. Une même personne doit pouvoir escorter N visiteurs en même temps. Ces visiteurs doivent alors tous badger dans un délai de Z secondes après le passage de l'escorte sous peine de déclencher une alarme. Au-delà de N visiteurs, deux personnels sont requis pour l'escorte, l'un passant en premier, l'autre en dernier. Le logiciel doit vérifier que tous les visiteurs escortés sont bien passés entre les deux accompagnateurs et déclencher une alarme si ce n'est pas le cas. Les personnels autorisés à accompagner des visiteurs doivent pouvoir être explicitement déclarés comme tels dans le système. Le système doit pouvoir refuser la fonction d'escorte aux personnels qui n'ont pas été explicitement déclarés comme étant autorisés à accompagner des visiteurs.

L2 Le logiciel doit permettre à un détenteur de droits particuliers de s'affranchir de la fonction « anti *pass-back* ». L'autorisation d'accès doit être accompagnée d'un message particulier traçant l'utilisation de ce privilège.

L2 Le logiciel doit permettre d'empêcher l'accès à une zone incluse dans une autre si la personne n'a pas préalablement badgé à l'entrée de la première zone.

Exemple : l'accès à la zone blanche n'est possible qu'après avoir badgé pour entrer dans la zone orange.



L3 Le logiciel doit posséder une fonction qui interdit l'accès à une zone, à une personne qui n'a pas été vue sortie de la zone où elle était préalablement localisée (cette fonction ne s'applique qu'aux zones ayant un lecteur en entrée ou en sortie).

L3 Le logiciel doit traiter le passage effectif : « la personne ayant badgé n'est considérée dans la zone que lorsqu'elle a vraiment pénétré dans cette zone, et non pas lors de la présentation de la carte d'accès ».

A4.9 Gestion des alarmes et événements

L1 La datation sera effectuée au plus près de l'évènement ou de l'alarme.

L1 Le logiciel doit rendre obligatoire la procédure d'acquittement des alarmes.

L1 Le système doit permettre de suivre l'évolution de l'état des alarmes : date et heure de l'apparition, description, localisation, date et heure de prise en compte par l'opérateur, date et heure de résolution.

L1 Le logiciel doit présenter les alarmes aux opérateurs dans l'ordre de priorité du niveau le plus élevé au plus faible.

L1 Une consigne spécifique pourra être attachée à chaque alarme. Cette consigne pourra être affichée à l'agent de protection à chaque apparition de l'alarme.

L1 Dans un site avec des zones incluses dans d'autres zones, on ne peut ouvrir une zone intermédiaire que si l'on a badgé dans les zones externes.

L2 Le logiciel doit traiter et afficher les alarmes en temps réel. Les alarmes doivent être différenciées des événements normaux du système (ex. : accès autorisé…).

L2 Le logiciel doit permettre d'imprimer les alarmes au fil de l'eau.

L2 Les éléments secrets maîtres du système (clés cryptographiques) devront être saisis manuellement ou injectés par le responsable sécurité du site et ne devront pas être générés par le système ni fournis par le fournisseur qui devra néanmoins apporter son assistance pour former l'intervenant à cette opération.

L3 Pas d'exigence spécifique pour ce niveau.

A4.10 Stockage et archivage

L1 Le logiciel doit permettre d'effectuer des archivages et stockages avec identification précise des périodes correspondant aux données.

L1 Les données du système seront idéalement stockées dans une base de données d'un format non propriétaire, dimensionnée de manière à pouvoir archiver au minimum 2 mois d'historique.

L2 Pas d'exigence spécifique pour ce niveau.

L3 Pas d'exigence spécifique pour ce niveau.

A4.11 Biométrie

L1 L'identification biométrique est acceptable.

L2 La biométrie ne peut venir qu'en complément d'un badge.

L3 L'usage d'un code, en complément obligatoire du badge, sera préférable à l'usage de la biométrie (non révocable).

A4.12 Installation

L1 Pas d'exigence spécifique pour ce niveau.

L2 Le système devra être installé par du personnel certifié par un organisme habilité, dans la mesure où un schéma de certification adéquat existe. Les certificats devront être présentés.

L3 Pas d'exigence spécifique pour ce niveau.

A4.13 Maintenance

L1 L'usage de la télémaintenance doit être conforme aux recommandations de l'ANSSI sur l'infogérance : http://www.ssi.gouv.fr/infogerance.

L2 La maintenance devra être assurée par du personnel certifié par un organisme habilité, dans la mesure où un schéma de certification adéquat existe. Les certificats devront être présentés.

L2 Les tiers en maintenance s'engagent à notifier la présence de vulnérabilités sur la version déployés des systèmes dont ils ont la responsabilité.

A minima ils proposeront les correctifs ou les mesures de contournement dans un délai de X heures/jours/semaines après leur publication par l'éditeur.

Idéalement ils s'engagent à déployer ses patchs et correctifs de sécurité après la mise à disposition par les fabricants des équipements concernés.

L2 Un suivi des versions majeures déployées des différents systèmes devra être fourni régulièrement (tous les Y mois). Ce suivi devra mettre en avant les différences entre les versions déployées et les versions compatibles avec le système les plus récentes.

L3 L'usage de la télémaintenance est fortement déconseillé.

Annexe 5 Contraintes règlementaires

Il est nécessaire que toutes les dispositions soient prises afin d'assurer prioritairement la sécurité des personnes en cas de catastrophes nécessitant des évacuations.

Certaines procédures sont également à effectuer auprès de la Commission nationale de l'informatique et des libertés (CNIL), dans le cadre de la protection de la vie privée, en fonction des dispositifs mis en place.

Pour finir, des contraintes plus spécifiques peuvent s'appliquer en fonction des zones protégées.

Cette annexe n'a pas pour vocation d'être exhaustive, mais de fournir un aperçu des contraintes à prendre en compte dans un projet de mise en place de systèmes de contrôle d'accès.

A5.1 Protection des personnes

En cas de catastrophes nécessitant une évacuation (des incendies la plupart du temps, mais également d'autres risques potentiels en fonction de l'environnement de travail), des procédures doivent être précisément définies. En particulier, le système doit pouvoir déverrouiller tous les accès concernés par l'alarme (bâtiment ou zone), afin que l'évacuation ne soit pas bloquée ou ralentie, et éditer la liste des personnes se trouvant à l'intérieur (cf. normes NFS 61-937 et NFS 61-931 sur les issues de secours).

Il appartient au responsable du site de définir les modalités de retour dans les locaux à l'issue d'une alerte :

- ouverture complète des points d'accès (nécessite alors un contrôle humain pour s'assurer que ceux qui rentrent en ont bien le droit) ;
- fonctionnement normal du système (il faut alors pouvoir réinitialiser le système).

En cas de panne d'un ou plusieurs composants du système, il appartient aussi au responsable du ou des sites de choisir quel doit être le fonctionnement dégradé du système en fonction des objectifs de sécurité, de la configuration du site et des capacités de l'organisme. Le comportement dégradé ne doit bien entendu pas perturber l'évacuation des personnes en cas de catastrophe. Le système pourra par exemple basculer en position « tout ouvert ». Mais ceci peut ne pas être du tout satisfaisant. Une autre solution pourrait être d'adjoindre une commande manuelle de déverrouillage depuis l'intérieur (selon le dispositif mécanique du point d'accès) permettant ainsi la sortie du personnel. Il faut alors traiter le cas de l'entrée d'individus avec le concours de personnels de sécurité.

Cela montre bien l'importance d'un système particulièrement redondant pour garantir la plus grande résilience possible.

A5.2 Norme simplifiée n°42 de la CNIL

La norme simplifiée n°42 de la CNIL concerne le traitement automatisé d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion d'accès au locaux, des horaires et de la restauration.

Cette norme simplifiée ne traite pas le cas des dispositifs utilisant des données biométriques (cf. 3.4.2 Utilisation de la biométrie par empreintes).

En général, les systèmes de contrôle d'accès utilisant des technologies sans contact relèvent, lorsqu'ils n'utilisent pas de techniques biométriques par empreintes, de cette norme simplifiée. Ils sont donc soumis à un régime de déclaration de conformité à cette norme.

Concernant la journalisation des événements, et conformément aux exigences de cette norme simplifiée, il est important de prendre en compte le fait que les éléments relatifs au déplacement des personnes ne peuvent être conservés au-delà de trois mois.

Pour finir, la CNIL fixe les règles quant au traitement des informations personnelles : communication et durée de conservation des éléments d'identification, information des usagers, etc. Ces règles sont consultables sur le site de la CNIL.

A5.3 Utilisation de la biométrie

Tous les traitements de données à caractère personnel, dès lors qu'ils mettent en jeu des données biométriques (empreinte, contour de la main, etc. et à l'exception de la biométrie par veines par exemple), doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

Dans les cas suivants, les formalités sont allégées et se réduisent à une déclaration de conformité à des « autorisations uniques » :

- cas des dispositifs reposant sur la reconnaissance du contour de la main et ayant pour finalité le contrôle d'accès ainsi que la restauration sur les lieux de travail (autorisation unique n°AU-007)[29].
- cas des dispositifs reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée (c'est-à-dire le badge et non l'UTL) et ayant pour finalité le contrôle d'accès aux locaux sur les lieux de travail (autorisation unique n°AU-008).

A5.4 Implication des instances représentatives du personnel

La mise en place d'un système de contrôle d'accès doit se faire en accord avec le Code du Travail, puisqu'elle implique un changement des conditions de travail.

La direction doit informer de son intention de mettre en place un contrôle des accès physiques, demander l'avis des instances représentatives du personnel (Comité hygiène et sécurité, Comité d'entreprise).

A5.5 Personnes à mobilité réduite

Lorsque les zones protégées sont susceptibles d'accueillir des personnes handicapées à mobilité réduite, il est important de prendre en compte la norme NF P 99-611 relative à l'accessibilité des personnes à mobilité réduite. Les têtes de lecture par exemple doivent être installées à une hauteur par rapport au sol de 1,10m à 1,30m par rapport au sol, ainsi que tout dispositif additionnel d'authentification (boitier de saisie de code PIN, d'empreinte biométrique, etc.).

A5.6 Autres

Attention, certaines zones protégées sont concernées par des réglementations particulières qui impacteront les caractéristiques du système de contrôle des accès.

C'est le cas par exemple des sites comportant des installations abritant des matières nucléaires, dont les systèmes d'information participant à la protection des zones névralgiques ne peuvent en aucun cas être interconnectés au réseau public, ni aux autres réseaux, sauf dispositions particulières.

On retrouve également d'autres contraintes réglementaires spécifiques pour les sites classés SEVESO[30], les zones ATEX[31], etc. Toutes ces contraintes doivent être clairement identifiées dès l'expression du besoin.

[29] Par délibération n°2012-322 du 20 septembre 2012 publiée au JORF n°0238 du 12 octobre 2012, la CNIL a mis fin à la possibilité de recourir à l'autorisation unique n°AU-007 pour les dispositifs reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion des horaires de travail. Les systèmes préalablement autorisés disposent d'un délai de 5 ans à partir de la publication pour se mettre en conformité.

[30] La directive 96/82/CE ou directive SEVESO est une directive européenne qui impose aux Etats membres d'identifier les sites industriels présentant des risques d'accidents majeurs.

[31] La règlementation ATEX (Atmosphères Explosives) est issue de deux directives européennes (94/9/CE et 1999/92/CE). Cette règlementation a été transposée en France dans le code du travail à l'article R 4227-50.

À propos de ce guide

Ce guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques a été réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Cette version de travail 1.0 est publiée à l'occasion du colloque « Contrôle des accès, comment faire les bons choix ? » organisé par le CNPP le 22 novembre 2012.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n°2009-834 du 7 juillet 2009 modifié par le décret n°2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur http://www.ssi.gouv.fr

Agence nationale de la sécurité des systèmes d'information

ANSSI – 51 boulevard de la Tour-Maubourg – 75 700 Paris 07 SP