RECOMMANDATIONS SUR LA SÉCURISATION DES SYSTÈMES DE CONTRÔLE D'ACCÈS PHYSIQUE ET DE VIDÉOPROTECTION

GUIDE ANSSI

ANSSI-PA-72
04/03/2020

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	19/11/2012	Version initiale
2.0	04/03/2020	Prise en compte des retours d'expérience, réorganisation des chapitres & refonte graphique

Table des matières

1
Introduction

Deuxième version du guide

La première version de ce guide sur la sécurité des technologies sans contact [1] pour le contrôle des accès physiques a été publiée en novembre 2012. Ce guide a pour principal objectif d'expliquer pourquoi les systèmes de contrôle d'accès doivent être considérés comme des systèmes d'information (SI) à part entière, relevant du périmètre de la Direction des systèmes d'information. Les retours d'expérience acquis depuis fin 2012 sur ces technologies ont incité l'ANSSI à publier une version actualisée de ce guide qui prend désormais aussi en compte les recommandations de sécurité pour la mise en œuvre de dispositifs de vidéoprotection issues de la note technique de l'ANSSI publiée en 2013 [8]. Les modifications apportées à la version initiale de ce guide incluent :

- une réorganisation des chapitres ;
- la prise en compte de la sécurité des systèmes de vidéoprotection ;
- un chapitre dédié à l'architecture des systèmes de contrôle d'accès et de vidéoprotection ;
- un changement de format pour faciliter la lisibilité des recommandations.

Ce guide se limite aux aspects d'architecture et de sécurité logique propres aux systèmes de contrôle d'accès utilisant des technologies sans contact, et aux systèmes de vidéoprotection. Comme lors de la rédaction du premier guide, l'ANSSI s'est associée au CNPP [2] pour mener une réflexion intégrant l'ensemble des éléments qui composent ces systèmes. Ce guide est ainsi complémentaire aux référentiels CNPP intitulés :

- « Référentiel APSAD D83 – Contrôle d'accès – Document technique pour la conception et l'installation » [28] ;
- « Référentiel APSAD R82 – Vidéosurveillance – Règle d'installation » [30] ;
- « Référentiel APSAD D32 – Cybersécurité – Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique » [29].

Le premier document 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, tandis que le deuxième document définit les exigences minimales auxquelles doivent répondre les installations de vidéoprotection. Enfin le dernier document définit les exigences techniques minimales auxquelles doivent répondre les systèmes de sécurité ou de sûreté raccordés à un réseau IP.

1. Les technologies sans contact dont il est fait mention dans ce guide s'appliquent aux technologies permettant l'identification d'un badge par une tête de lecture sans nécessité d'un contact physique entre les deux éléments.

2. Acteur de référence en prévention et en maîtrise de risques opérationnels intervenant dans les domaines de la sécurité incendie et explosion, de la sûreté et malveillance, de la cybersécurité, de l'atteinte à l'environnement et des risques professionnels. Se reporter à `https://www.cnpp.com`.

Objectifs

Ce guide se veut une aide à la décision quant au choix d'un système de contrôle d'accès sans contact ou de vidéoprotection, et propose les bonnes pratiques de sécurité pour leurs mises en œuvre. Il fournit des recommandations permettant d'assurer la mise en place de ces systèmes respectant un niveau de sécurité à l'état de l'art. Ces recommandations s'appliquent aussi bien à des systèmes de contrôle d'accès et de vidéoprotection « mono-site » qu'à des systèmes « multi-sites » dont la gestion est centralisée.

Pour les sites où ces systèmes sont déjà déployés, 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 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 ni pour les produits de vidéoprotection.

Information

Les recommandations formulées dans ce guide ne prennent aucun caractère obligatoire sauf si le contexte dépend d'une règlementation particulière.

Convention de lecture

Certains sujets abordés font l'objet de plusieurs recommandations qui se distinguent par leur niveau de sécurité. Le lecteur a ainsi la possibilité de choisir une solution en adéquation avec ses besoins en sécurité.

Dans une démarche itérative de sécurisation, les différents niveaux de sécurité proposés peuvent permettre de fixer une cible d'architecture et d'identifier les étapes pour l'atteindre.

Ainsi, les recommandations sont présentées de la manière suivante :

- R*x* constitue une recommandation à l'état de l'art ;
- R*x* - et R*x* - - constituent des recommandations alternatives à R*x*, d'un niveau de sécurité moindre et données dans l'ordre décroissant.

Par ailleurs, pour chacune des recommandations de ce guide, l'utilisation du verbe « *devoir* » signifie qu'il s'agit soit d'une exigence règlementaire, soit d'une exigence dont la mise en œuvre est impérative. La formulation « *il est recommandé* » est utilisée pour tout ce qui relève des bonnes pratiques.

Publics ciblés

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 ou de vidéoprotection, que ce soit dans une entreprise privée ou un organisme public ;
- aux acheteurs, qui pourront imposer dans leurs appels d'offres les exigences détaillées en annexe D 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 pourront s'intéresser aux aspects liés à l'exploitation et la maintenance du système.

Les objectifs de ces différents acteurs peuvent être différents. Le tableau ci-dessous permet d'identifier les chapitres qui concernent plus particulièrement chacun d'entre eux :

Acteurs	**Chapitres recommandés**
Chefs de projet, Personnes en charge de la mise en place d'un système de contrôle d'accès sans contact	Chapitre 2 : Composants du contrôle d'accès et de la vidéoprotection Chapitre 3 : Étapes préliminaires Chapitre 4 : Architecture Chapitre 5 : Cartographie Chapitre 6 : Sécurité des éléments support du contrôle d'accès Chapitre 7 : Sécurité des éléments support de vidéoprotection Chapitre 8 : Autres éléments de sécurité Chapitre 9 : Principes cryptographiques
Acheteurs	Annexe D : Spécifications
Installateurs, Intégrateurs	Chapitre 2 : Composants du contrôle d'accès et de la vidéoprotection Chapitre 4 : Architecture Chapitre 5 : Cartographie Chapitre 6 : Sécurité des éléments support du contrôle d'accès Chapitre 7 : Sécurité des éléments support de vidéoprotection Chapitre 8 : Autres éléments de sécurité Chapitre 9 : Principes cryptographiques Chapitre 10 : Identification, authentification et droits d'accès
Exploitants	Chapitre 10 : Identification, authentification et droits d'accès Chapitre 11 : Administration Chapitre 12 : Maintenance et exploitation Chapitre 13 : Journalisation et supervision

TABLE 1.1 – Public ciblé

2
Composants du contrôle d'accès et de la vidéoprotection

2.1 Composants du contrôle d'accès physique

2.1.1 Définition d'un système de contrôle d'accès physique

Système de contrôle d'accès physique

Un système de contrôle d'accès physique 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 contrôlées aux seules personnes qui ont le droit d'y accéder.

Un système de contrôle d'accès physique 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 supports principaux interviennent :

- le badge [4] (ou support similaire) ;
- 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 centre de gestion du système.

3. La fonction de traçabilité des accès est assurée dans le cadre du traitement des données.
4. Par souci de facilitation de la lecture, le terme « badge » sera utilisé de façon générique pour désigner tout type de support.

2.1.2 Description des composants d'un système de contrôle d'accès physique

Badge

Un badge est un type d'identifiant utilisé dans les systèmes de contrôle d'accès. Dans la suite de ce guide, nous considérons que le badge intègre des technologies sans contact.

Tête de lecture

Une tête de lecture est un dispositif relais permettant de communiquer d'une part avec le badge au travers des technologies sans contact, et d'autre part avec une unité de traitement local. Une tête de lecture peut être associée à un clavier ou à un lecteur biométrique.

Unité de traitement local

Une unité de traitement local (UTL) est un dispositif qui assure la gestion de plusieurs têtes de lecture, commande et contrôle l'état de plusieurs ouvrants, chacun étant associé à une ou plusieurs têtes de lecture. Les UTL sont paramétrées et gérées depuis le centre de gestion des contrôles d'accès.

Centre de gestion des contrôles d'accès

Le centre de gestion des contrôles d'accès, également appelé GAC[5], est une infrastructure centralisée assurant notamment :

- la centralisation des journaux d'événements ;
- l'affichage et la notification des événements à l'opérateur ;
- l'hébergement et la mise à jour de la base de données centrale (droits, utilisateurs, groupes, identifiants de badge, etc.) ;
- le pilotage de l'ensemble des UTL ainsi que la transmission périodique de la base de données nécessaire au traitement local des demandes d'accès.

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

Station de gestion

La station de gestion désigne le poste de travail à partir duquel l'opérateur du GAC effectue les opérations d'exploitation et d'administration du système de contrôle d'accès.

5. Gestion des accès contrôlés. On notera que le GAC est aussi appelé unité de traitement de supervision (UTS).

Station d'enrôlement

La station d'enrôlement désigne le poste de travail à partir duquel un opérateur effectue les opérations d'enrôlement des badges.

Liaison filaire

Une liaison filaire désigne le câblage mis en place pour raccorder une tête de lecture à une UTL [6].

Réseau support

Un réseau support désigne le commutateur sur lequel sont connectées des UTL (cf. figure 2.1).

Réseau fédérateur

Un réseau fédérateur désigne l'ensemble des équipements réseau intervenant dans la mise en relation entre les réseaux support et le réseau du GAC (cf. figure 2.1).

Logiciel de gestion du système

Un logiciel de gestion du système est une couche applicative, installée sur le serveur de gestion du GAC, dont le rôle est de communiquer de manière logique avec des UTL et donc de les piloter.

2.1.3 Description des différentes phases du contrôle d'accès

Identification/authentification

Les notions d'identification et authentification utilisées dans ce guide sont conformes à celles définies par l'ANSSI telles qu'exprimées dans le référentiel général de sécurité [17]. 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/authentification peut se réduire seulement à l'identification du badge, ou à l'identification et l'authentification du badge. Le cas le plus complet inclut l'identification, l'authentification du badge et l'authentification du porteur.

6. le cas de la connectivité sans fil est traité dans la section 4.2 de ce document.

Traitement des demandes d'accès

Le traitement des demandes d'accès est assuré en premier lieu par l'UTL. Cette unité assure la gestion de toutes les demandes d'accès en provenance des têtes de lecture qui lui sont rattachées, analyse ces demandes vis-à-vis d'un ensemble de droits d'accès stocké dans sa base de données locale et délivre les commandes de déverrouillages.

Verrouillage et déverrouillage

Le dispositif de verrouillage permet de réaliser le blocage mécanique d'un point d'accès pour empêcher le passage des personnes non autorisées. Le contrôle d'accès permet le déverrouillage. Dans le cadre d'une analyse de risque, il convient de prendre en compte les situations dégradées (coupure électrique) et les cas d'ouverture automatique (incendie). Ces procédures d'exploitation particulières sont traitées dans la section 12.4 de ce guide.

2.2 Composants de la vidéoprotection

2.2.1 Définition d'un système de vidéoprotection

Système de vidéoprotection

Un système de vidéoprotection est un système composé de moyens d'acquisition, de transmission, de gestion et d'enregistrement d'images ayant pour objectif la protection de sites, de bâtiments ou de locaux à distance.

Un système de vidéoprotection assure plusieurs fonctions de base :

- prise de vues ;
- gestion et visualisation des images ;
- enregistrement et rendu des images ;
- gestion des alarmes ;
- journalisation des activités.

D'autres fonctions comme la commande de caméras orientables sont susceptibles d'être gérées par le système de vidéoprotection.

Toutes ces fonctions sont assurées par les éléments support principaux que sont la caméra et le centre de gestion vidéo.

2.2.2 Description des composants d'un système de vidéoprotection

Caméra

Une caméra est un dispositif opérant dans le visible ou dans l'infrarouge qui permet l'acquisition d'images. Les caméras sont de deux types, numériques ou analogiques. Elles peuvent aussi être classées en deux catégories :

- les caméras fixes ;
- les caméras orientables [7].

Boîtier de conversion analogique-numérique

Un boîtier de conversion analogique-numérique est un dispositif permettant de convertir les signaux des caméras analogiques en signaux numériques transmis au travers du protocole TCP/IP à destination du centre de gestion vidéo.

Centre de gestion vidéo

Un centre de gestion vidéo, aussi appelé VMS (*Video management system*), est l'infrastructure de gestion assurant la centralisation des images et la gestion des caméras. Ce centre inclut principalement un ou plusieurs serveurs, une capacité de stockage, des équipements réseau, et des équipements de sécurité. Le VMS est susceptible d'assurer tout ou partie des fonctionnalités suivantes :

- commande des caméras orientables ;
- commande des fonctions de visualisation des images ;
- enregistrement des images ;
- visualisation des images en direct ou en différé ;
- analyse vidéo intelligente (traitement d'images) ;
- gestion des droits d'utilisation et d'accès ;
- journalisation d'activité et supervision ;
- gestion d'alarmes vidéos.

Station de gestion

Une station de gestion désigne le poste de travail à partir duquel l'opérateur du VMS effectue les opérations d'exploitation et d'administration du système de vidéoprotection. Des dispositifs d'orientation des caméras de type *joystick* sont souvent associés à la station de gestion.

7. Les caméras orientables sont soit dotées de fonctions panoramiques, d'inclinaison et de zoom auquel cas elles sont aussi appelées caméras PTZ (*pan-tilt-zoom*), soit dotées de fonctions de balayage horizontal et vertical auquel cas elles sont aussi appelées caméras PT (*pan-tilt*).

Liaison filaire

Une liaison filaire désigne le câblage mis en place pour raccorder les caméras analogiques aux boîtiers de conversion analogique-numérique.

Réseau support

Un réseau support désigne le commutateur réseau sur lequel sont connectées des caméras IP ou des boîtiers de conversion analogiques-IP (cf. figure 2.1).

Réseau fédérateur

Un réseau fédérateur désigne l'ensemble des équipements réseaux intervenant dans la mise en relation entre les réseaux support avec le réseau du centre de gestion (cf. figure 2.1).

2.3 Schéma général

La figure 2.1 représente un exemple d'architecture de système de contrôle d'accès physique et de système de vidéoprotection. L'architecture présentée dans cet exemple est purement illustrative ; elle servira de référence tout au long de ce guide. Les éléments suivants figurant sur le schéma qui n'ont pas été présentés dans ce chapitre le seront dans la suite de ce guide :

- les pare-feux en section 4.4 ;
- les VPN en section 4.4.

Les petites clés de couleur présentes sur le schéma 2.1 illustrent la diversité des clés cryptographiques mises en œuvre dans un SI de contrôle d'accès physique et de vidéoprotection.

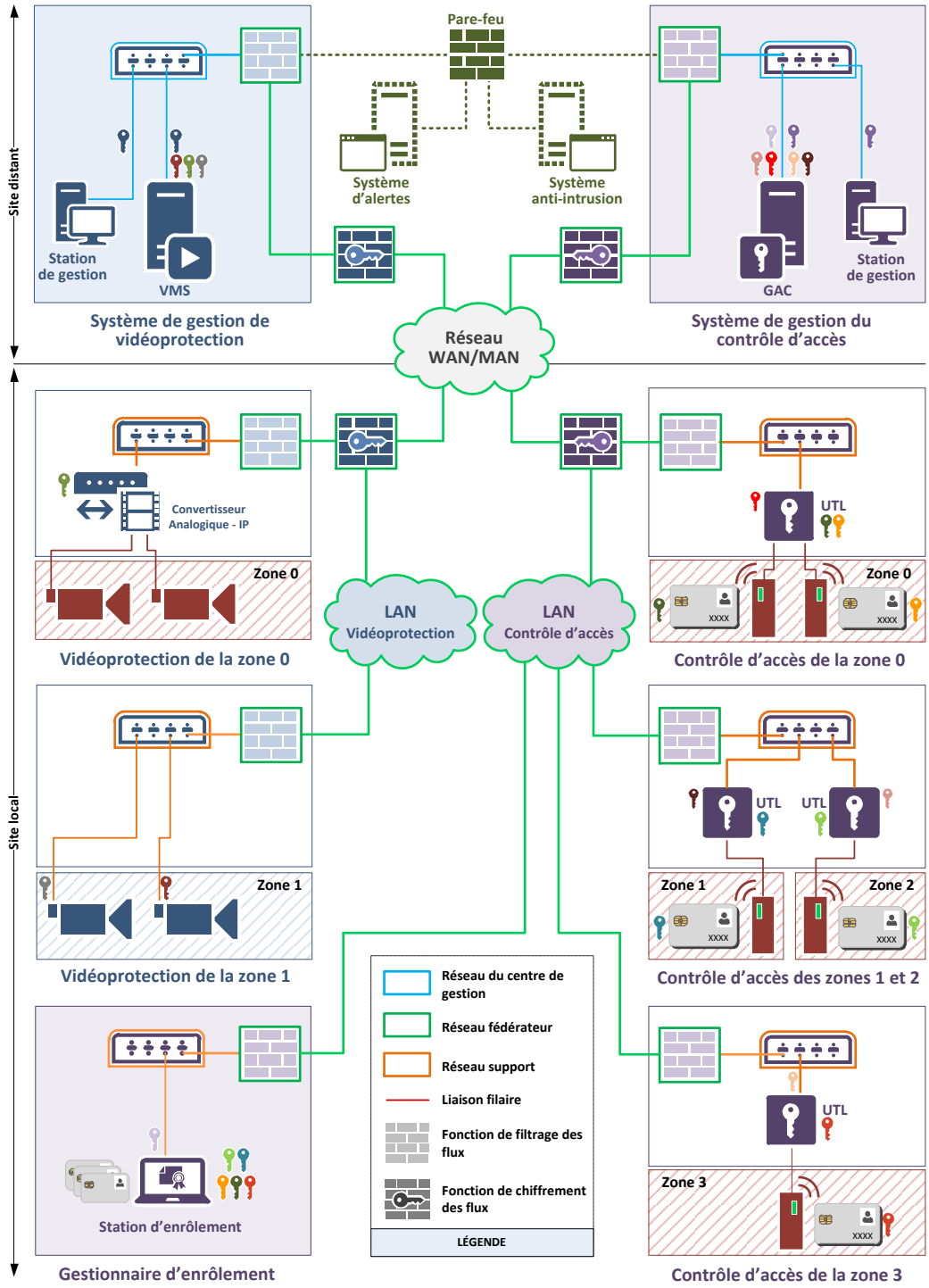

FIGURE 2.1 – Exemple d'architecture générale

2.4 Produits qualifiés par l'ANSSI

La qualification [23] prononcée par l'ANSSI permet d'attester d'un certain niveau de sécurité et de confiance dans les produits [8]. Ce processus permet de s'assurer notamment que des produits remplissent les objectifs de sécurité définis dans des cibles de sécurité préalablement approuvées.

R1

Privilégier l'utilisation de produits qualifiés par l'ANSSI

D'une manière générale, il est recommandé que les matériels et les logiciels utilisés pour le contrôle d'accès physique et la vidéoprotection soient qualifiés par l'ANSSI au niveau requis par les besoins de sécurité. À défaut, il est recommandé qu'ils disposent d'un autre Visa de sécurité délivré par l'ANSSI [9].

Attention

Il est recommandé d'être toujours attentif aux versions de matériel ou logiciel auxquelles les Visas de sécurité s'appliquent, ainsi qu'à la définition de la cible de sécurité.

8. La qualification des produits par l'ANSSI comporte trois niveaux : élémentaire, standard et renforcé.
9. Se reporter à `https://www.ssi.gouv.fr/visa-de-securite`.

3
Étapes préliminaires à la mise en place d'un système de contrôle d'accès ou de vidéoprotection

Pour bien appréhender les besoins de sécurité relatifs au contrôle d'accès physique ou à la vidéoprotection, 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/contrôler ;
- les valeurs métier [10] et biens supports [11] à protéger ;
- les zones incluses dans chaque site ainsi que leurs niveaux de protection attendus ;
- les flux de circulation des individus entre les zones ;
- les acteurs ;
- les processus organisationnels.

Certains de ces aspects ne sont évoqués que sommairement dans ce guide. Les lecteurs qui souhaiteraient accéder à plus d'information peuvent se référer aux référentiels du CNPP :

- « APSAD D83 – Contrôle d'accès – Document technique pour la conception et l'installation » [28] ;
- « APSAD R82 – Vidéosurveillance – Règle d'installation » [30].

3.1 Identification des sites à protéger/contrôler

L'identification détaillée des sites à protéger/contrôler est une étape importante préalable à la mise en place d'un système de contrôle d'accès physique ou de vidéoprotection. Cette étape permet de clarifier les contraintes qui pèsent sur le projet et de disposer des éléments nécessaires, entre autres, à la rédaction des appels d'offres. 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 :

10. Les « valeurs métier » définies dans la méthode EBIOS-RM [12] correspondent aux « biens essentiels » de la méthode EBIOS 2010 [14]. Il est utile de faire une distinction entre les valeurs métier qui, dans un système d'information, sont des biens immatériels (informations ou processus utiles à la réalisation des missions de l'organisme), et les biens supports dont ils dépendent pour le traitement, le stockage ou la transmission.

11. Les biens support définis dans la méthode EBIOS-RM [12] correspondent aux composantes du SI sur lesquelles reposent une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle.

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

R2

Identifier les sites à protéger/contrôler

Il est nécessaire de référencer de manière exhaustive les sites à contrôler en prenant en compte leurs particularités.

3.2 Identification des valeurs métier et biens supports à protéger

Une fois les sites référencés, il convient d'identifier les valeurs métier et les biens supports à protéger. Cette identification, menée dans le cadre d'une analyse de risque, doit permettre également de définir le niveau de sensibilité de chaque site au regard du cadre règlementaire susceptible de leur être associé.

D'une manière générale, les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour atteindre ses objectifs [12].

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

L'ANSSI publie une méthode d'appréciation et de traitement des risques proposant notamment des outils permettant de recenser l'ensemble des valeurs métier et des biens supports : la méthode EBIOS *Risk Manager* [12].

R3

Identifier les valeurs métier et les biens supports à protéger

Il est recommandé d'identifier, au travers d'une analyse de risque, les valeurs métier et les biens supports sur lesquels elles s'appuient, pour déterminer les ressources qu'il convient de protéger, et définir le niveau de sensibilité associé à chaque site référencé.

12. Définition extraite du guide EBIOS *Risk Manager* [12].

3.3 Identification de zones

Après avoir réalisé l'inventaire des valeurs métier, des biens supports et de leur localisation, l'étape suivante consiste à distinguer des zones avec différents niveaux de protection attendus au sein des sites identifiés.

Niveau de protection attendu

Le niveau de protection attendu est associé au niveau de criticité des biens sensibles présents dans la zone. Plus les biens sensibles présents dans cette zone seront critiques, plus le niveau de protection attendu associé à la zone sera important.

Zone contrôlée

Une zone contrôlée est une zone *a priori* fermée, dont tous ses accès sont équipés de lecteurs de badges, ou placés sous vidéoprotection.

Il est recommandé d'établir une échelle précise et explicite des niveaux de protection attendus, avec leurs définitions associées. La numérotation à partir de zéro est tout à fait indiquée pour cet usage, le niveau 0 étant alors la zone considérée comme semi-publique, à l'intérieur de la limite de propriété.

Les niveaux de protection attendus supérieurs (1, 2, etc.) correspondent aux zones contrôlées, entourées de barrières physiques comprenant un nombre restreint de points d'accès, et situées dans l'enceinte des sites ou des bâtiments. Les niveaux de protection attendus les plus élevés correspondent aux zones névralgiques.

R4

Définir les zones incluant les systèmes de contrôle d'accès ou de vidéoprotection au niveau de protection attendu le plus élevé

Les zones où sont situés les éléments du système de contrôle d'accès ou de vidéoprotection (serveurs du centre de gestion du système, et stations de travail) doivent être définies au niveau de protection attendu le plus élevé.

Les sites à protéger doivent être découpés en zones classées par niveau de protection attendu selon l'échelle préalablement conçue. Ces zones n'ont pas à être découpées selon la configuration physique existante des lieux, mais bien selon le niveau de criticité des biens sensibles présents dans la zone : un tel projet peut nécessiter de conduire des travaux de réorganisation de cloisons, de bâtiments et de sites afin que la sécurité physique puisse être optimisée voire même rendue possible.

Si plusieurs zones sont regroupées pour ne former plus qu'une seule zone, la nouvelle zone ainsi formée sera du niveau de protection attendu égal au niveau de protection attendu le plus élevé des zones regroupées.

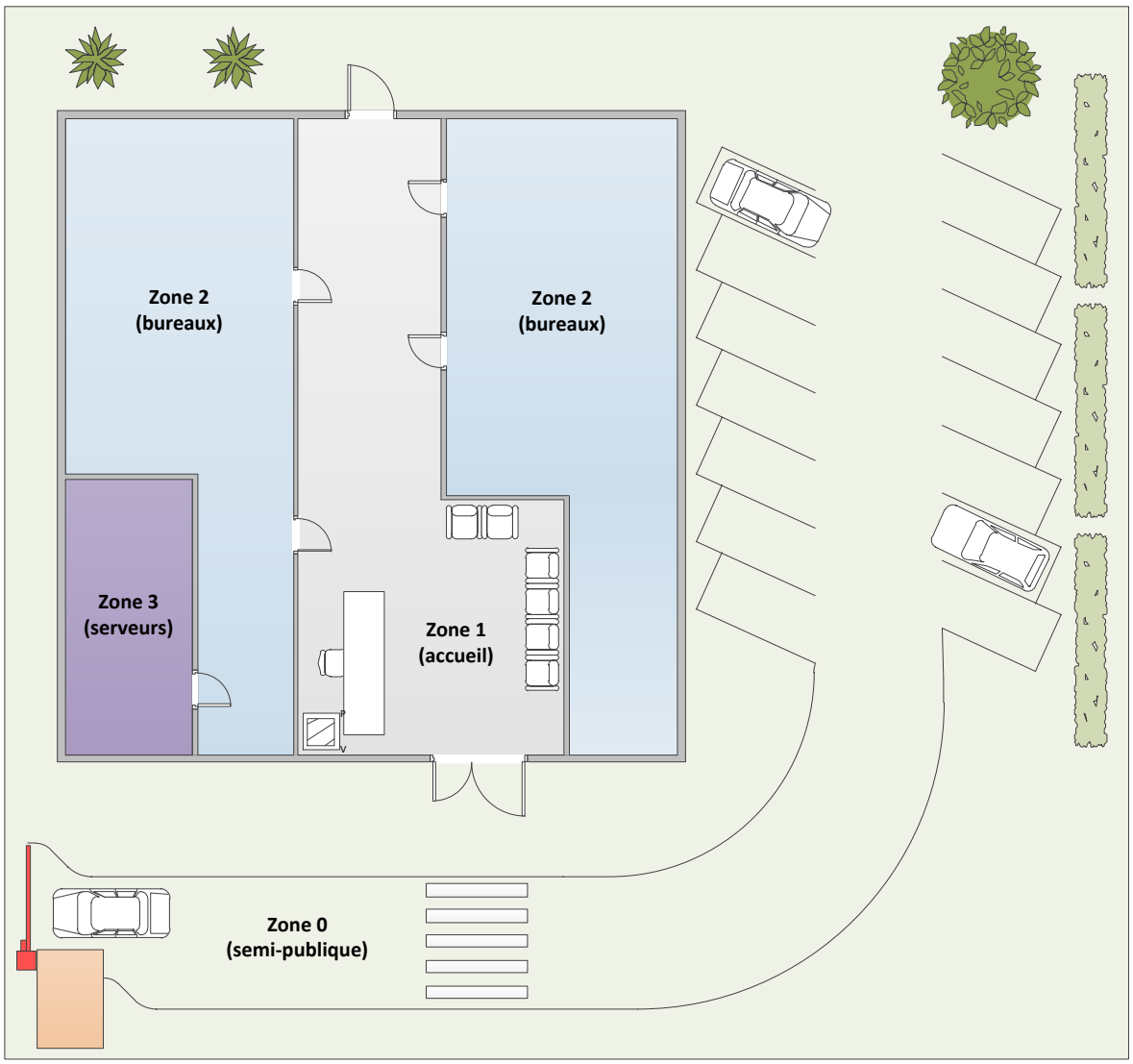

FIGURE 3.1 – Exemple de découpage d'un site en zones associées à des niveaux de protection attendus

Sur le plan de bâtiment reproduit en figure 3.1, ont été représentées quatre zones de niveaux de protection attendus différents :

- zone semi-publique de niveau 0, accessible potentiellement à tout le monde mais destinée aux visiteurs et placée sous vidéoprotection ;
- zone d'accueil de niveau 1, accessible aux employés munis d'un badge et aux visiteurs autorisés au moyen d'un contrôle visuel au niveau de la réception ;
- zone de bureaux de niveau 2, accessible aux seuls employés et aux visiteurs accompagnés munis d'un badge.
- salle serveurs de niveau 3, accessible aux seuls employés autorisés et aux visiteurs accompagnés,

et authentifiés au moyen d'un badge et d'un second facteur.

R5

Identifier les zones avec leurs niveaux de protection attendus

Il est recommandé qu'une échelle précise et explicite des niveaux de protection attendus avec leurs définitions associées soit établie. Il est ensuite recommandé que les sites à protéger soient découpés en zones classées par niveau de protection attendu selon cette échelle.

3.4 Niveau de sûreté des équipements et des installations de contrôle d'accès physique

Le niveau de sûreté des équipements et des installations de contrôle d'accès physique 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 protection attendu des zones précédemment définies.

Ces niveaux de sûreté et types de menaces présentés dans le tableau 3.1 ont été définis en lien avec le CNPP. Ce même tableau est reproduit dans le référentiel « APSAD D83 » [28] :

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, etc.)	Pas de connaissance	I
Franchissement par attaque mécanique 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 fabriquant ou les distributeurs	II
Franchissement par attaque mécanique 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 ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées	Matériel comprenant des moyens de cryptanalyse ou maquette électronique spécifique conçue 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 fabriquant	IV

TABLE 3.1 – Les quatre niveaux de sûreté

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

R6

Identifier les niveaux de sûreté adaptés aux menaces des sites

Il est recommandé qu'une analyse de risque soit menée afin d'identifier, pour chaque site à contrôler, les niveaux de sûreté des équipements et installations de contrôles d'accès physique 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 et pourquoi ? 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'urgence, etc.) ;
- les plages horaires ;
- les exigences particulières de circulation et contraintes spécifiques (ex. : sorties de secours) ;
- la quantité prévisionnelle de passages.

Les réponses à ces questions permettent de déduire les chemins de circulation et les mesures de sécurité qu'il convient de mettre en place en fonction des types de passage à contrôler. Trois exemples de flux physiques ont été représentés sur un plan de bâtiment (cf. figure 3.2), montrant les principales personnes extérieures intervenant au sein des locaux et leurs déplacements autorisés.

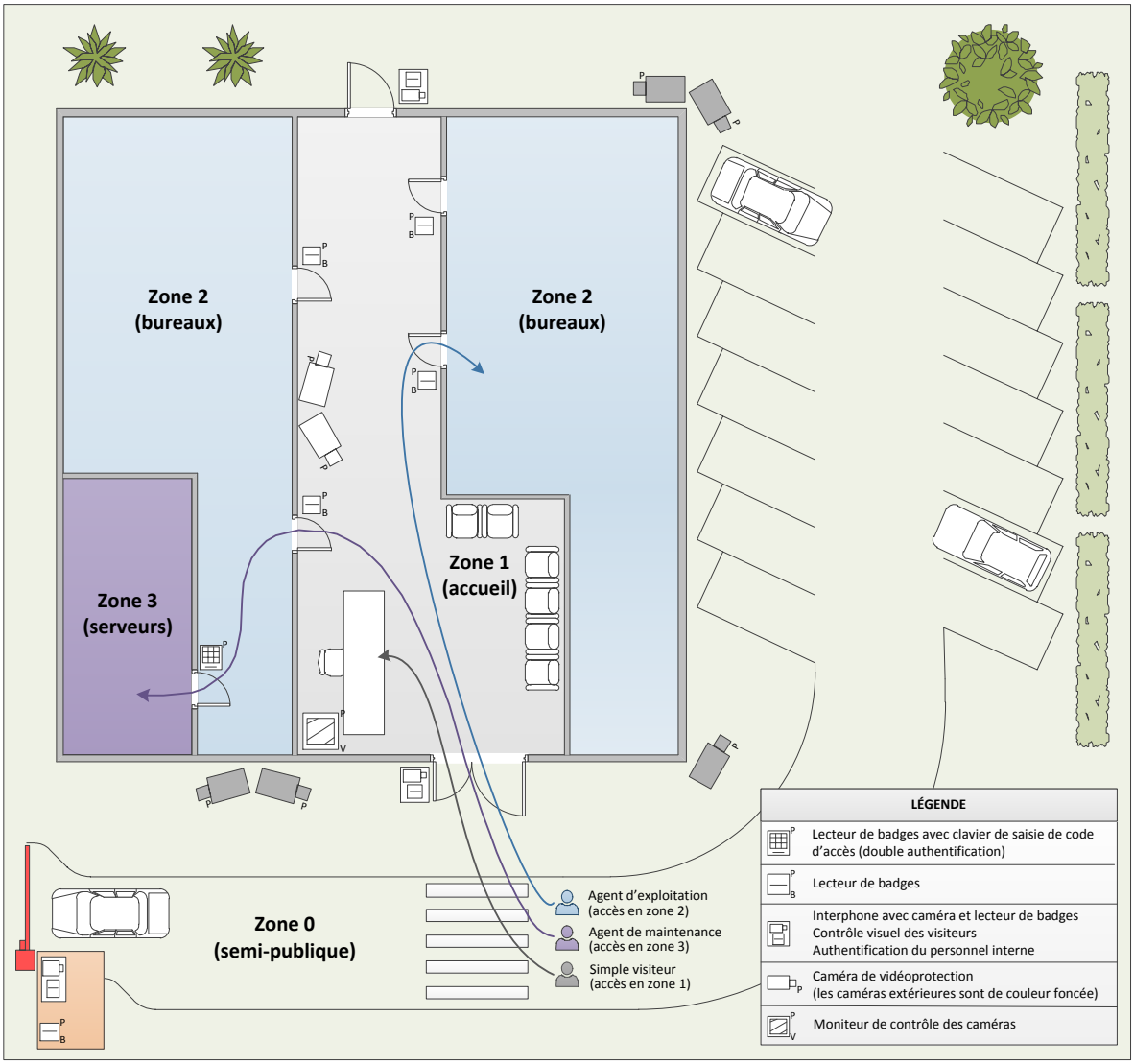

FIGURE 3.2 – Exemple de flux physiques

R7

Identifier les flux de circulation des individus

Dans le but de connaître les besoins de chaque point d'accès à contrôler, il est recommandé d'identifier les flux de circulation des individus.

3.6 Identification des acteurs

Différents rôles peuvent être distingués parmi les intervenants dans les processus organisationnels de gestion des accès physiques et de vidéoprotection :

- les demandeurs (service de gestion des ressources humaines, responsables hiérarchiques, 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 GAC ;
- les opérateurs du VMS ;
- les opérateurs de sauvegarde des systèmes ;
- les opérateurs d'exploitation des journaux d'événements des systèmes ;
- les mainteneurs des matériels physiques, qui interviennent sur la partie matérielle ;
- les administrateurs applicatifs [13], qui effectuent les opérations de maintenance sur les applications ;
- les administrateurs techniques, qui effectuent les opérations de maintenance sur les systèmes d'exploitation ;
- les usagers ou porteurs de badge.

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. De plus, il faut éviter que la gestion du système soit dépendante d'une seule personne potentiellement défaillante.

R8

Identifier les acteurs

Les différents acteurs intervenant dans les processus organisationnels de gestion des accès physiques et de vidéoprotection doivent être clairement identifiés pour que leurs droits d'accès soient calculés au plus juste. Dans les cas où plusieurs rôles sont susceptibles d'être assurés par les mêmes personnes, il faut s'assurer de la pertinence des droits résultant de ces cumuls (voir la section 10.4).

3.7 Processus organisationnels

Les processus organisationnels doivent être clairement déterminés dès l'expression des besoins. Il s'agit de formaliser 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 d'accès d'un badge ;
- modification de droits d'utilisation et d'accès aux vidéos.

13. Une attention toute particulière doit être portée à la sécurité du système lorsqu'il est fait appel à la télémaintenance (voir la section 12.6.2 consacrée à ce sujet).

Un exemple type de ces processus est donné en annexe B.

L'absence de processus organisationnels est généralement source d'approximations dans la gestion des badges (délivrance, révocation), dans la pertinence des droits d'accès affectés aux usagers, et dans l'attribution des droits d'utilisation aux opérateurs VMS/GAC.

R9

Définir les processus organisationnels liés à la gestion des accès physiques et de la vidéoprotection

Il est fortement recommandé que les processus organisationnels décrivant les échanges entre les acteurs de la gestion des accès physiques et de la vidéoprotection pour la réalisation d'un objectif particulier soient clairement définis et formalisés.

4
Architecture d'un système de contrôle d'accès et de vidéoprotection

La conception d'une architecture autour des systèmes de contrôle d'accès ou de vidéoprotection repose sur l'identification des zones à contrôler, associées à des niveaux de protection attendus. Cette étape, décrite dans le chapitre précédent (cf. section 3.3), doit être complétée par l'identification des zones considérées comme sensibles ou soumises à la règlementation [14]. Ces zones doivent être protégées/contrôlées par un SI de contrôle d'accès physique ou de vidéoprotection de sensibilité identique, ou soumis à la même règlementation.

Une zone contrôlée peut inclure des têtes de lecture, des caméras, des liaisons filaires, des UTL ou des convertisseurs analogiques/IP. Ces dispositifs sont regroupés au sein de réseaux support, eux même interconnectés aux centres de gestion au travers du réseau fédérateur. Une zone contrôlée est donc associée à un ou plusieurs réseaux support, sachant qu'il est envisageable dans certains cas qu'un réseau support contienne des dispositifs issus de plusieurs zones présentant des niveaux de protection attendus différents. La mutualisation d'équipements évoquée dans ce dernier point ne doit être considérée qu'au regard de l'analyse de risque liée à la mise en place de l'infrastructure de contrôle d'accès ou de vidéoprotection.

Après la phase d'identification des zones à contrôler, la démarche à suivre pour l'élaboration d'une architecture de contrôle d'accès ou de vidéoprotection est la suivante :

- identifier le nombre de systèmes de contrôles d'accès ou de vidéoprotection à mettre en place en fonction de la sensibilité des zones à traiter ;
- déterminer l'emplacement des centres de gestion ;
- déterminer à partir de l'analyse de risque les dispositifs liés à des zones de niveaux de protection attendus différents qui peuvent être mutualisés sur un même réseau support ;
- déterminer le ou les réseaux fédérateurs qui véhiculeront les flux de contrôle d'accès ou de vidéoprotection jusqu'aux centres de gestion ;
- déterminer les interconnexions nécessaires entre les centres de gestion et les autres SI de l'entité ;
- déterminer l'emplacement des stations d'enrôlement et des stations de gestion.

Parallèlement à cette démarche, il convient d'appliquer un certain nombre de règles de sécurité décrites en détail dans ce chapitre dont la mise en œuvre aura un impact sur l'architecture globale.

Ces règles sont regroupées en six thèmes principaux exposés en liaison avec la démarche décrite plus haut :

14. II901 [20], IGI1300 [15], etc.

- SI de contrôle d'accès et de vidéoprotection ;
- liaison filaire ;
- réseau support ;
- réseau fédérateur ;
- architecture s'appuyant sur un service externalisé ;
- interconnexion.

Un exemple d'élaboration d'une architecture de contrôle d'accès et de vidéoprotection est donnée dans l'annexe C. Cet exemple suit la démarche indiquée dans cette introduction et s'appuie sur les schémas et illustrations qui figurent dans ce guide.

4.1 SI de contrôle d'accès et de vidéoprotection

Les dispositifs de contrôle d'accès et de vidéoprotection présentent des niveaux d'exposition souvent élevés compte tenu de leur emplacement et de leur accessibilité. Ces dispositifs représentent donc une porte d'entrée significative pour une intrusion dans le système d'information de l'entité, notamment lorsque le réseau support ou le réseau fédérateur de ces dispositifs est partagé avec d'autres composants du SI. Les SI liés au contrôle d'accès physique et à la vidéoprotection doivent donc être considérés comme des SI à part entière, distincts du SI de l'entité.

R10

Cloisonner physiquement les SI de contrôle d'accès et de vidéoprotection

Les SI de contrôle d'accès et de vidéoprotection doivent être cloisonnés des autres composantes du système d'information de l'entité. Il est hautement recommandé qu'un cloisonnement physique (câblage et équipements réseau dédiés) soit privilégié par rapport à un cloisonnement logique (VLAN par exemple), dont le niveau de robustesse peut être insuffisant dans ce contexte.

R10 -

Cloisonner logiquement les SI de contrôle d'accès et de vidéoprotection

A défaut d'un cloisonnement physique, il est recommandé de cloisonner logiquement les SI de contrôle d'accès et de vidéoprotection par rapport aux autres composantes du SI de l'entité en mettant en œuvre des mécanismes de filtrage, de chiffrement et d'authentification de réseau reposant sur le protocole IPsec. La mise en œuvre du protocole IPsec doit être conforme aux recommandations du guide de l'ANSSI [9].

Si des zones considérées comme sensibles, ou soumises à la règlementation, sont identifiées parmi les zones qui doivent être contrôlées, il faut dédier un système complet de contrôle d'accès physique ou de vidéoprotection pour chaque niveau de sensibilité identifié.

R11

Dédier un SI de contrôle d'accès ou de vidéoprotection pour chaque niveau de sensibilité identifié

Lorsque l'architecture globale inclut des zones de sensibilités différentes, les zones de même sensibilité doivent bénéficier d'un SI de contrôle d'accès ou de vidéoprotection qui leur est dédié. Il faut dans ce cas considérer chaque ensemble de même sensibilité comme un SI à part entière.

4.2 Liaison filaire

4.2.1 Protection des liaisons filaires

La particularité d'un lecteur de badge réside dans le fait qu'il est situé à l'extérieur de la zone contrôlée. Ce lecteur étant rattaché à l'UTL par une liaison filaire, l'accès à cette liaison filaire peut permettre à un attaquant d'atteindre directement l'équipement situé en amont, à savoir l'UTL. Dans le cas d'une caméra extérieure, la liaison filaire qui connecte la caméra au réseau support (ou au convertisseur analogique/IP s'il s'agit d'une caméra analogique) peut présenter une partie apparente pouvant être exploitée par un attaquant pour atteindre des équipements placés en amont.

R12

Protéger les liaisons filaires

Il est recommandé que les liaisons filaires ne soient ni apparentes, ni situées dans une zone non contrôlée. Dans le cas des liaisons filaires associées aux caméras extérieures, elles doivent être si possible non apparentes et protégées physiquement (encastrées, bien enterrées, etc.).

4.2.2 Connexions entre les têtes de lecture et l'UTL

Comme indiqué dans la section précédente, les têtes de lecture sont des dispositifs très vulnérables de par leur emplacement situé à l'extérieur de la zone contrôlée. Il convient d'être vigilant quant aux possibilités d'actions malveillantes qui permettraient, depuis une tête de lecture, d'accéder aux autres têtes de lecture connectées sur la même UTL.

R13

Privilégier des connexions point-à-point entre les têtes de lecture et l'UTL

Il est recommandé de privilégier la mise en place de connexions point-à-point [15] sur les liaisons entre les têtes de lecture et l'UTL.

L'UTL étant le dispositif le plus proche d'une tête de lecture, il convient de s'assurer de l'homogénéité des degrés d'exposition des têtes de lecture qui lui sont rattachées.

15. Une connexion point-à-point est une connexion directe sans équipement intermédiaire de commutation ou de concentration.

R14

Respecter l'homogénéité des degrés d'exposition des têtes de lecture rattachées à une UTL

Une UTL ne doit desservir que des têtes de lecture contrôlant l'accès à des zones dont le niveau de protection attendu est identique.

4.2.3 Connectivité filaire et connectivité sans-fil

Une connectivité filaire est à privilégier pour les dispositifs de contrôle d'accès physique, comme pour les dispositifs de vidéoprotection. En effet, même si certaines têtes de lecture ou certaines caméras supportent différents modes de communication sans-fil (ZigBee [16], Wi-Fi ou téléphonie 3G essentiellement), la mise en œuvre de ces fonctionnalités n'est pas recommandée car elles augmentent très significativement l'exposition des dispositifs aux attaques logiques [17].

R15

Privilégier une connectivité filaire pour les dispositifs de vidéoprotection et de contrôle d'accès physique

Il est fortement recommandé de privilégier la connectivité filaire à la connectivité sans-fil pour les dispositifs de vidéoprotection comme pour les dispositifs de contrôle d'accès physique.

R15 -

Activer un deuxième chiffrement dans le cas d'une connectivité sans-fil

Dans le cas où le choix de la liaison sans-fil est obligatoire, il est recommandé de s'orienter vers des solutions proposant un deuxième chiffrement, en plus du chiffrement opéré par la liaison sans-fil. Les flux doivent être authentifiés, et protégés en confidentialité et en intégrité. Les opérations de chiffrement et de déchiffrement doivent s'effectuer en zone contrôlée. La borne d'accès sans-fil doit être placée à l'intérieur de la zone contrôlée.

4.3 Réseau support

4.3.1 Segmentation au sein du réseau support

Les dispositifs de contrôle d'accès physique ou de vidéoprotection situés sur un même réseau support ont la possibilité de communiquer entre eux au sein de ce réseau. Cette possibilité de communication accroît fortement la surface d'attaque de ces dispositifs puisqu'il est alors possible pour un attaquant d'atteindre tous les dispositifs à partir de l'interface réseau d'un de ces équipements.

R16

Cloisonner logiquement les dispositifs au sein du réseau support

Il est fortement recommandé de mettre en œuvre un cloisonnement logique entre les dispositifs au sein du réseau support. En particulier, dans la mesure où les différents dispositifs n'ont pas de raison légitime de communiquer entre eux directe-

16. Protocole de communication sans-fil à courte portée et faible consommation reposant sur la norme IEEE 802.15.4.
17. Il convient d'être très vigilant quant à la disponibilité des liaisons sans-fil au regard notamment du positionnement de l'antenne et des possibilités de brouillage.

ment, il est recommandé de configurer les commutateurs réseau de telle sorte que chaque dispositif ne puisse établir de communication qu'avec les serveurs de gestion, et en aucun cas avec les autres dispositifs. Un tel cloisonnement peut par exemple être obtenu par la mise en œuvre sur les commutateurs réseau d'un mécanisme d'isolation de type PVLAN [18], empêchant les communications directes entre dispositifs, voire de VLAN filtrés et dédiés à chaque dispositif s'il s'agit d'une infrastructure de taille limitée. Des recommandations sur la mise en œuvre de ces cloisonnements sont indiquées dans le guide de l'ANSSI sur la sécurisation d'un commutateur de desserte [2].

4.3.2 Contrôle des accès directs au réseau support

La prévention des accès illégitimes au réseau support doit s'appuyer sur un contrôle des points d'accès physiques, en évitant de laisser des ports apparents et accessibles (ex. : prise réseau murale pour le raccordement d'une caméra IP sur le réseau support).

R17

Ne pas laisser les points d'accès au réseau apparents

Les points d'accès au réseau des dispositifs comme les UTL ou les caméras constituant une vulnérabilité, il est recommandé qu'ils ne soient ni apparents ni accessibles facilement.

Une pratique efficace pour se protéger contre les intrusions consiste à désactiver les ports inutilisés des commutateurs réseaux.

R18

Désactiver les ports inutilisés sur les commutateurs réseau

Les ports inutilisés sur les commutateurs réseau doivent être désactivés.

Les ports non désactivés doivent être protégés contre la connexion de matériel illégitime en lieu et place d'un dispositif existant. Lorsque les dispositifs le supportent, il est souhaitable d'imposer une authentification cryptographique des accès au réseau, par exemple par la mise en œuvre du protocole 802.1X pour le contrôle d'accès aux ports réseau, voire par le contrôle des adresses MAC des dispositifs connectés.

R19

Contrôler les accès aux ports réseau par authentification

Afin de limiter les possibilités d'accès illégitimes au réseau via le port d'accès d'un équipement, il est recommandé de mettre en œuvre une authentification cryptographique des accès au réseau comme le protocole 802.1X, dans la mesure où les dispositifs connectés supportent ce protocole. Dans ce cas, il est recommandé que le déploiement du réseau 802.1X s'appuie sur les recommandations mentionnées dans le guide de l'ANSSI sur sa mise en œuvre [3].

18. *Private VLAN*. Ce mécanisme d'isolation est décrit dans le document [32].

R19 -

Contrôler les accès aux ports réseau par vérification des adresses MAC

Dans le cas où les dispositifs ne supportent pas le protocole 802.1X, il est recommandé, par défaut, que les accès aux ports réseau soient contrôlés par la vérification de la légitimité des adresses MAC des dispositifs qui se connectent.

4.3.3 Mutualisation des dispositifs de contrôle d'accès physique sur un même réseau support

La mutualisation de plusieurs UTL sur un même réseau support n'est possible que si les UTL concernées sont associées à des zones dont le niveau de protection attendu est identique. La mutualisation au sein d'un même réseau support d'UTL associées à des zones de niveaux de protection attendus différents ne peut être envisagée que si cette mutualisation est prise en compte dans l'analyse de risque. Il faut privilégier dans ce cas la mise en œuvre d'un cloisonnement logique entre les UTL associées à des zones de niveaux de protection attendus distincts.

R20

Cloisonner logiquement au sein d'un réseau support les UTL associées à des zones de niveaux de protection attendus distincts

Lorsque l'analyse de risque prévoit la mutualisation au sein d'un même réseau support de dispositifs de contrôle d'accès physique associés à des zones de niveaux de protection attendus distincts, il est recommandé de mettre en place un cloisonnement logique (ex. : VLAN) entre ces dispositifs.

4.3.4 Mutualisation des dispositifs de contrôle d'accès physique et de vidéoprotection sur un même réseau support

La mutualisation des dispositifs de contrôle d'accès physique et de vidéoprotection sur un même réseau support présente un risque élevé au regard du positionnement de certaines têtes de lecture à l'extérieur du périmètre à contrôler. En effet, au-delà de la différence de finalités et des rôles complémentaires de ces deux types de dispositifs, leurs niveaux d'exposition à des atteintes physiques sont souvent différents. C'est le cas par exemple lorsque les caméras de vidéoprotection sont positionnées exclusivement à l'intérieur de la zone contrôlée, tandis que certains lecteurs de badges sont par construction à l'extérieur de celle-ci.

La figure 4.1 montre un exemple de mutualisation à éviter dans la mesure où les dispositifs de contrôle d'accès physique et les dispositifs de vidéoprotection partagent le même support physique, même s'il serait possible de les isoler logiquement :

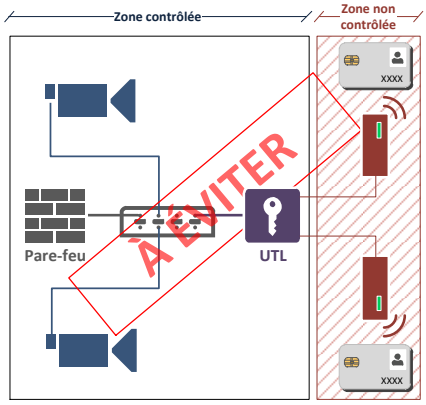

FIGURE 4.1 – Exemple à éviter de mutualisation du réseau support

La figure 4.2 illustre un exemple recommandé où les dispositifs de vidéoprotection et de contrôle d'accès physique ont leur propre réseau support :

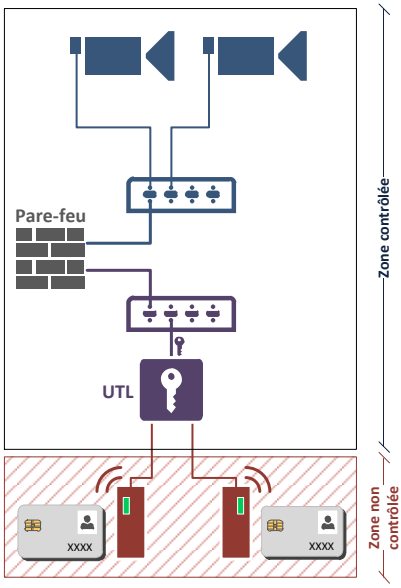

FIGURE 4.2 – Exemple recommandé de réseaux support non mutualisés

R21

Éviter de mutualiser les dispositifs de contrôle d'accès et de vidéoprotection sur un même réseau support

Il est recommandé de ne pas mutualiser sur un même réseau support les dispositifs de contrôle d'accès physique et ceux associés à la vidéoprotection.

Un cloisonnement logique peut néanmoins être envisagé si les dispositifs concernés contrôlent des zones dont le niveau de protection attendu est identique.

R21 -

Mettre en place un cloisonnement logique entre les dispositifs de contrôle d'accès et de vidéoprotection mutualisés sur un même réseau support

Lorsque la mutualisation de dispositifs de vidéoprotection et de contrôle d'accès physique sur des réseaux support communs s'avère incontournable et que les zones contrôlées par ces dispositifs nécessitent un même niveau de protection, il est recommandé de mettre en place un cloisonnement logique (ex. : VLAN) entre ces dispositifs.

Information

Il est à noter que la zone intitulée « non controlée » délimitée en rouge sur les schémas de ce chapitre correspond dans la plupart des cas à une zone contrôlée de niveau de protection attendu inférieur au niveau de protection attendu de la zone intitulée « zone contrôlée » délimitée en bleu sur les schémas.

4.3.5 Réseau support des caméras placées à l'extérieur de la zone contrôlée

Dans une architecture de vidéoprotection incluant un réseau de caméras situées à l'extérieur de la zone contrôlée et un réseau de caméras situées à l'intérieur de la zone contrôlée, il convient d'être vigilant sur les possibilités d'intrusion dans le système de vidéoprotection depuis la zone extérieure. En effet, les caméras extérieures étant par nature plus exposées, une action malveillante sur celles-ci ne doit pas permettre de porter atteinte à la confidentialité des flux circulant dans les zones contrôlées. Il convient donc de bien cloisonner le réseau support des caméras extérieures des autres réseaux support dédiés aux caméras internes, comme illustré sur la figure 4.3 :

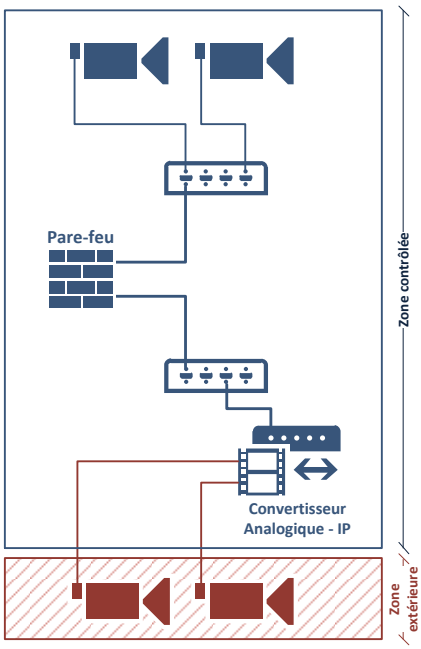

FIGURE 4.3 – Exemple recommandé de réseau support dédié aux caméras extérieures

R22

Dédier physiquement un réseau support pour les caméras extérieures

Il est recommandé de déployer les caméras situées en dehors de la zone contrôlée sur un réseau support physiquement dédié et distinct des autres réseaux support incluant les caméras situées dans la zone contrôlée.

Si cette recommandation est difficilement applicable compte tenu du contexte, une alternative de sécurité moindre peut être envisagée sur la base d'un cloisonnement logique.

R22 -

Cloisonner logiquement le réseau des caméras extérieures

A défaut d'un cloisonnement physique, les caméras situées en dehors de la zone contrôlée doivent être déployées sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de cloisonnement logique, de filtrage, de chiffrement et d'authentification de réseau (IPsec). La mise en œuvre du protocole IPsec doit être conforme aux recommandations du guide de l'ANSSI [9].

4.4 Réseau fédérateur

Les recommandations énoncées dans cette section concernent les réseaux fédérateurs des systèmes de contrôle d'accès physique et de vidéoprotection, chacun pris séparément.

4.4.1 Filtrage des flux entre les réseaux support

Lorsque plusieurs réseaux support sont raccordés sur un réseau fédérateur commun à l'image de l'exemple en figure 4.4, les communications entre les réseaux support doivent être réduites aux seuls flux nécessaires au fonctionnement du système. En effet, une connexion sans aucun filtrage faciliterait la compromission d'un réseau support à partir d'un autre réseau support compromis.

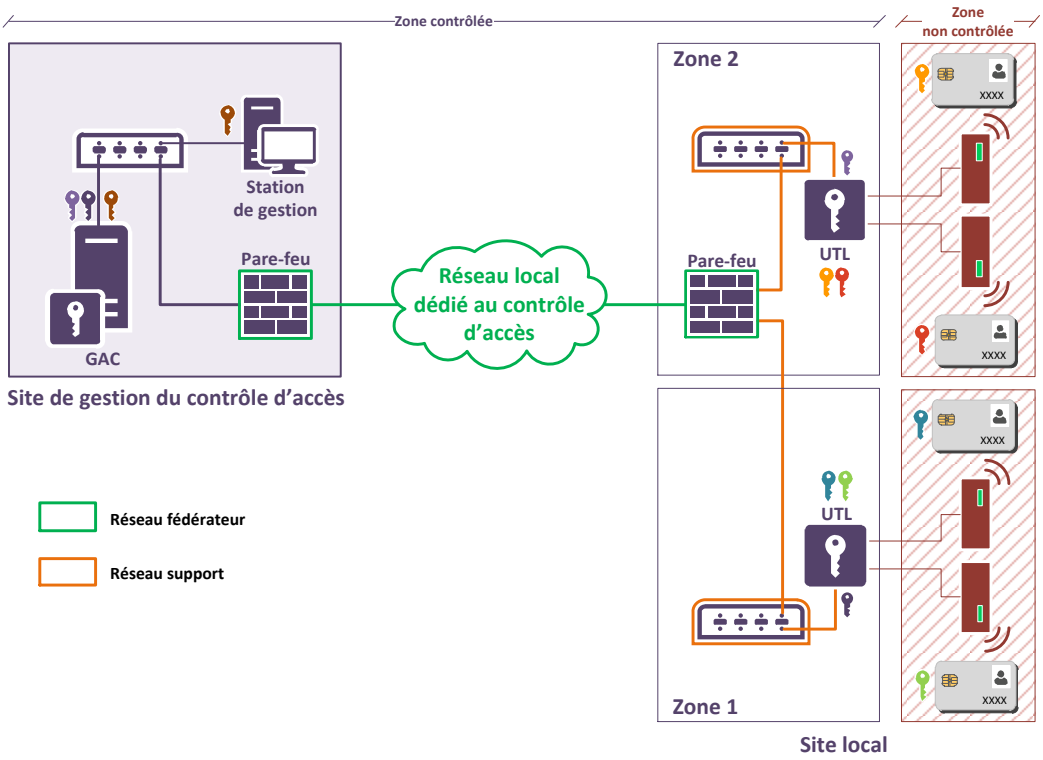

FIGURE 4.4 – Exemple d'architecture incluant plusieurs réseaux support

R23

Filtrer les flux entre les réseaux support

Les flux en provenance et à destination des réseaux support doivent être filtrés par un ou plusieurs pare-feux. Il est recommandé de bloquer par défaut tous les flux entre les réseaux support et de n'autoriser que les flux strictement nécessaires au fonctionnement du système.

4.4.2 Filtrage des flux entre les réseaux support et le réseau du centre de gestion

Les réseaux support communiquent avec le réseau du centre de gestion au travers d'un réseau fédérateur à l'image de l'exemple en figure 4.4. Afin de limiter les risques de compromission du centre de gestion depuis un réseau support compromis, les flux échangés entre les réseaux support et le réseau du centre de gestion doivent être filtrés.

R24

Filtrer les flux entre les réseaux support et le réseau du centre de gestion

Il est recommandé que les flux échangés entre les réseaux support et le centre de gestion soient filtrés par un pare-feu positionné en amont du centre de gestion. Ce pare-feu doit être configuré pour :

- s'assurer que les flux échangés n'utilisent que les protocoles autorisés ;
- s'assurer que les flux sont échangés uniquement entre équipements autorisés.

4.4.3 Infrastructure répartie sur plusieurs sites

Dans certains cas de figure, les dispositifs de contrôle d'accès physique ou de vidéoprotection peuvent être éloignés de leur centre de gestion respectif. Les flux transitent alors potentiellement par des réseaux de transport non maîtrisés par l'entité. Le réseau de transport peut également comporter des parties exposées (cas d'un site s'étendant sur plusieurs hectares), la notion de maîtrise du réseau de transport est alors laissée à l'appréciation de l'entité. Il est nécessaire dans tous les cas de protéger les flux en confidentialité et en intégrité. La figure 4.5 montre un exemple d'infrastructure répartie sur plusieurs sites où les flux issus des dispositifs de contrôle d'accès physique doivent transiter au travers d'un réseau non maîtrisé.

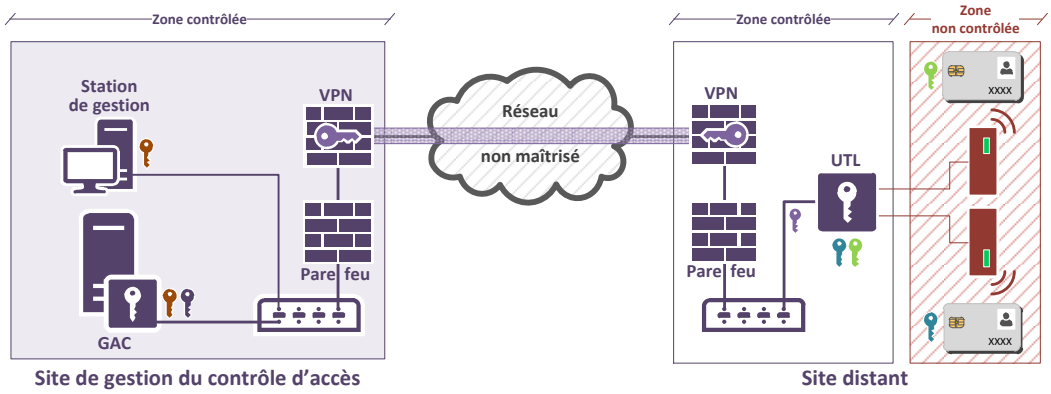

FIGURE 4.5 – Exemple de réseau fédérateur reposant sur un réseau de transport non maîtrisé

R25

Protéger les flux de contrôle d'accès et de vidéoprotection transitant par un réseau de transport non maîtrisé

Si les flux de contrôle d'accès ou de vidéoprotection en provenance de sites distants circulent sur un réseau de transport non maîtrisé, ces flux doivent être chiffrés et authentifiés depuis le site distant jusqu'au site où est localisé le centre de gestion correspondant. Dans ce cas, un tunnel IPsec entre les sites concernés doit être établi conformément aux recommandations du guide de l'ANSSI [9].

4.5 Architecture s'appuyant sur un service externalisé

Dans le cas où le serveur de gestion de contrôle d'accès ou de vidéoprotection est externalisé sur un service d'informatique en nuage ou chez un prestataire de services, il convient d'être très vigilant sur le niveau de sécurisation des services qui sont proposés. L'exemple d'architecture en figure 4.6 illustre un service de gestion de vidéoprotection hébergé sur un service d'informatique en nuage, mais qui pourrait être aussi bien hébergé chez un prestataire de services.

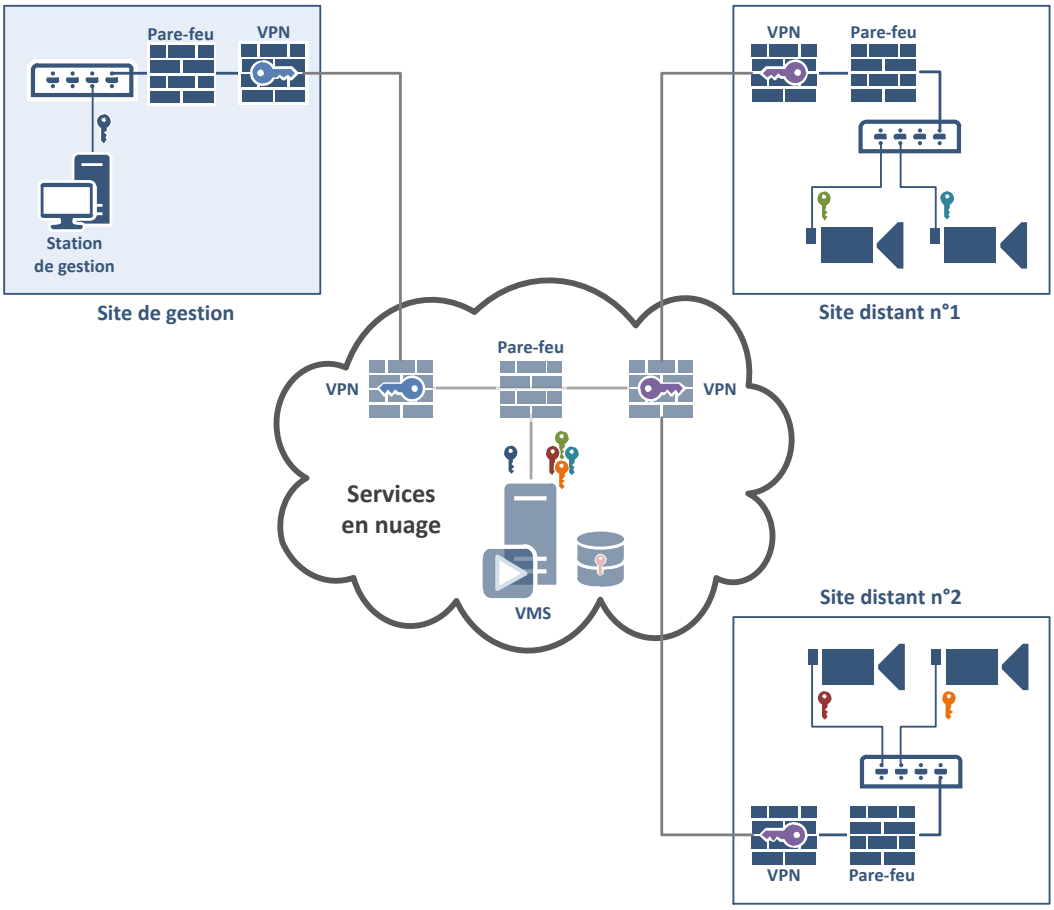

FIGURE 4.6 – Exemple d'architecture incluant l'hébergement du serveur de gestion de vidéoprotection sur un service d'informatique en nuage

Ce type d'architecture est toutefois à éviter. En effet, le risque de compromission des éléments secrets stockés dans un environnement non maîtrisé est accru, de même que le risque lié à la confidentialité des données qui y sont déposées.

R26

Éviter l'externalisation des services de gestion chez un prestataire de services

Il est recommandé d'éviter de recourir à l'externalisation des services de gestion de contrôle d'accès ou de vidéoprotection chez un prestataire de services.

Si toutefois l'entité fait le choix d'externaliser des services de gestion dans un service d'informatique en nuage ou chez un prestataire de services, il est recommandé que cette offre de service soit qualifiée par l'ANSSI selon le référentiel d'exigences SecNumCloud [22]. L'entité pourra également s'appuyer sur le guide d'externalisation des SI de l'ANSSI [4].

R26 -

Choisir un prestataire de services qualifié

Si l'externalisation des services de gestion du contrôle d'accès ou de vidéoprotection sur un service d'informatique en nuage ou chez un prestataire de services s'avère incontournable, il est recommandé que le choix du prestataire de services

s'oriente vers un prestataire qualifié par l'ANSSI selon le référentiel d'exigences SecNumCloud [22].

Information

Les prestataires de services d'informatique en nuage (SecNumCloud) sont référencés sur le site de l'ANSSI [19].

4.6 Interconnexion

Les systèmes de contrôle d'accès physique et de vidéoprotection ne sont généralement pas autonomes. Dans ce cas, des ouvertures vers d'autres SI sont nécessaires, ce qui a des impacts en matière de sécurité. Ces systèmes doivent donc satisfaire à des contraintes supplémentaires et les interconnexions avec d'autres SI (système de gestion des ressources humaines, etc.) doivent être étudiées avec soin.

4.6.1 Interconnexion entre un système de contrôle d'accès physique et le SI de l'entité

Les interconnexions entre un système de contrôle d'accès physique et le SI de l'entité doivent être étudiées minutieusement en raison de l'augmentation de la surface d'attaque induite par l'ouverture du système de contrôle d'accès physique sur le SI de l'entité. L'augmentation de la surface d'attaque concerne à la fois le SI du contrôle d'accès (réseau du centre de gestion potentiellement accessible depuis un équipement du SI de l'entité) et le SI de l'entité (équipements de ce SI potentiellement accessibles depuis le SI de contrôle d'accès). Les raisons justifiant la mise en place de telles interconnexions sont guidées par les besoins fonctionnels voire règlementaires. Les interconnexions les plus fréquemment rencontrées sont les suivantes :

- interconnexion avec le système de gestion des ressources humaines ;

  Cette interconnexion est soumise à la règlementation. Elle doit être mentionnée dans le registre des activités de traitement des données à caractère personnel de l'entité [20], à la fois dans la fiche relative au traitement de données du système de contrôle d'accès et dans la fiche relative au traitement des données du système de ressources humaines. Cette interconnexion peut 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 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 dans la mesure où la direction des ressources humaines a connaissance généralement en avance de la date du départ d'un collaborateur. 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 ne coïncide souvent pas avec l'ensemble des personnes recensées dans le SI des ressources humaines.

19. https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/.

20. Le registre des activités de traitement est défini dans l'article 30 du RGPD, Règlement général sur la protection des données entré en application le 25 mai 2018 [26].

- interconnexion avec le système de contrôle du temps de travail ;

  Cette interconnexion est soumise à la règlementation. Elle doit être mentionnée dans le registre des activités lié au traitement des données [20] dans le système de contrôle d'accès, ainsi que dans le registre des activités lié au traitement des données dans le système de contrôle du temps de travail. De plus, les instances représentatives du personnel doivent être informées ou consultées préalablement à la mise en place d'une telle interconnexion (cf. le mémo de la CNIL [21] sur l'accès aux locaux et le contrôle des horaires [24]).

- interconnexion avec les systèmes d'alertes en cas de catastrophe.

  L'interconnexion avec les systèmes d'alertes (c'est-à-dire d'incendie dans la plupart des cas) est une obligation règlementaire (voir l'annexe E). En cas d'incendie par exemple, le système doit pouvoir déverrouiller tous les accès concernés par l'alerte.

Ces interconnexions offrent souvent la possibilité de joindre le GAC depuis des éléments du réseau du SI de l'entité, ou de joindre des services disponibles sur le réseau du SI de l'entité depuis le GAC voire depuis les dispositifs connectés sur les réseaux support.

R27

Éviter une interconnexion avec le SI de l'entité

Dans la mesure du possible, il est recommandé d'éviter d'interconnecter le système de contrôle d'accès physique avec le SI de l'entité.

R27 -

Filtrer les accès au GAC depuis le SI de l'entité

Dans le cas où une interconnexion entre le GAC et un serveur du SI de l'entité serait incontournable, il est recommandé de filtrer tous les accès entre le GAC et le SI de l'entité. Seuls les flux concernés par le besoin d'interconnexion doivent être autorisés.

Les flux échangés entre un système de contrôle d'accès physique et le SI de l'entité contiennent des informations sensibles. Il convient donc de bien s'assurer que ces flux soient protégés en intégrité et en confidentialité.

R28

Protéger les flux échangés entre le système de contrôle d'accès et le SI de l'entité

Il est recommandé que les flux échangés entre un système de contrôle d'accès physique et le SI soient protégés en intégrité, authenticité et en confidentialité à l'aide de protocoles cryptographiques éprouvés comme TLS ou, mieux, IPsec.

Information

Les recommandations de sécurité pour la mise en œuvre des protocoles TLS ou IPsec sont décrites dans deux guides de l'ANSSI, le « Guide TLS » [10] et dans le guide « Recommandations de sécurité relatives à IPsec pour la protection des flux réseau » [9].

21. Commission nationale de l'informatique et des libertés - `https://www.cnil.fr`.

4.6.2 Interconnexion entre un système de contrôle d'accès physique et un système de vidéoprotection

L'interconnexion d'un système de contrôle d'accès physique avec un système de vidéoprotection est envisageable si la sécurisation des deux systèmes respecte les recommandations émises dans ce chapitre et, si les zones couvertes par les deux systèmes sont homogènes. Deux cas peuvent se présenter :

- interconnexion entre les deux centres de gestion ;
  Ce cas illustré en figure 4.7 suppose que les systèmes de contrôle d'accès physique et de vidéoprotection ont leur propre serveur de gestion, et que les deux serveurs de gestion sont interconnectés au travers des deux réseaux fédérateurs.

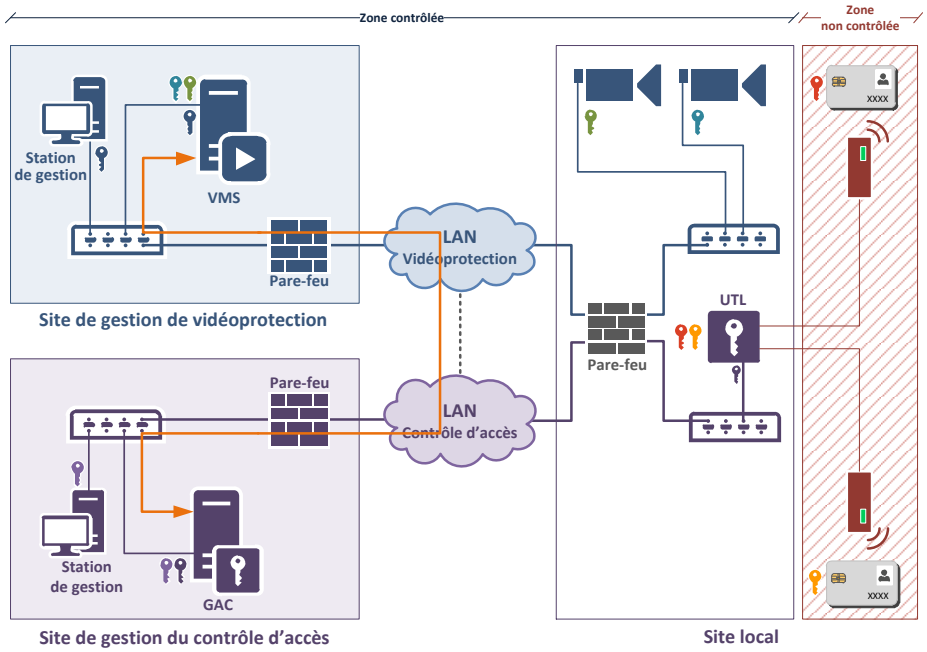

FIGURE 4.7 – Exemple d'interconnexion entre deux serveurs de gestion

- utilisation d'un centre de gestion commun aux deux systèmes.
  Ce cas illustré en figure 4.8 suppose que les systèmes de contrôle d'accès physique et de vidéoprotection partagent le même centre de gestion, et le même réseau fédérateur.

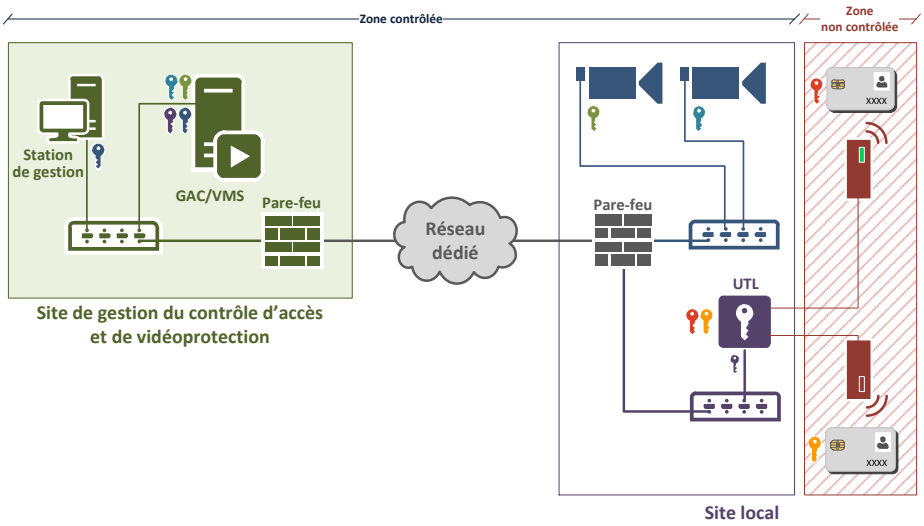

FIGURE 4.8 – Exemple de mutualisation des fonctions de gestion sur un seul serveur

La solution reposant sur des centres de gestion et des réseaux fédérateurs distincts pour chaque système permet un meilleur cloisonnement des flux liés à chaque système. Donc, en cas de compromission de l'un des deux systèmes, cette solution offre une meilleure sécurisation du système n'ayant pas été compromis.

La séparation des fonctions de gestion peut aussi être recherchée pour des raisons de sécurité, dans le cas où les logiciels de gestion sont identiques mais où la mutualisation des deux fonctions sur un seul centre de gestion n'est pas souhaitée. C'est également le cas où l'administration des deux systèmes est confiée à deux prestataires distincts.

R29

Privilégier une solution s'appuyant sur deux centres de gestion distincts

Dans le cas où des échanges entre des systèmes de contrôle d'accès et de vidéoprotection sont nécessaires, il convient de privilégier une solution s'appuyant sur deux centres de gestion et deux réseaux fédérateurs distincts avec une interconnexion entre les deux centres de gestion. Il est recommandé dans ce cas de chiffrer et d'authentifier les flux entre les deux centres de gestion et de n'autoriser que les flux métier strictement nécessaires.

La mutualisation des fonctions de gestion sur un seul centre de gestion peut apporter des fonctionnalités supplémentaires par l'association des images avec les informations attachées aux badges. Cette mutualisation se caractérise par un logiciel de gestion commun aux systèmes de contrôle d'accès physique et de vidéoprotection.

Dans le cas où cette solution est envisagée, le risque de compromission de ce centre de gestion est accru puisqu'il peut provenir des dispositifs et équipements des deux systèmes. Il faut donc bien s'assurer que les flux en provenance des réseaux support des deux systèmes et transitant par le réseau fédérateur sont filtrés et que seuls les flux strictement nécessaires sont autorisés.

R29 -

Filtrer les flux entre les réseaux support et le réseau du centre de gestion commun

Si l'utilisation d'un centre de gestion commun aux systèmes de contrôle d'accès et de vidéoprotection s'avère incontournable, il faut s'assurer que les recommandations R23 sur le filtrage des flux entre les réseaux support et R24 sur le filtrage des flux entre les réseaux support et le réseau du centre de gestion sont bien appliquées.

5
Cartographie

La cartographie est un outil essentiel à la maîtrise d'une infrastructure de contrôle d'accès et de vidéoprotection. Elle doit donc être établie et maintenue tout au long du cycle d'existence de ces SI. L'ANSSI a dédié un guide à ce sujet intitulé « Cartographie du SI » [11]. Les informations présentées dans ce chapitre sont extraites de ce guide, et adaptées aux contextes particuliers du contrôle d'accès physique et de la vidéoprotection. La cartographie se décompose en trois vues qui vont progressivement du métier vers la technique.

5.1 Vision métier

La vision métier a pour objectif de décrire l'ensemble des processus métiers avec les acteurs qui y participent. Les éléments suivants sont inclus *a minima* dans la vision métier :

- document détaillant les processus organisationnels ;
- document décrivant la liste des acteurs.

5.2 Vision applicative

La vision applicative décrit les solutions technologiques qui supportent les processus métier. Cette vision comprend les composants logiciels d'un système de contrôle d'accès physique ou de vidéoprotection, ainsi que les flux de données entre ces composants, mais aussi les périmètres et les niveaux de privilèges des utilisateurs et des administrateurs. Les éléments suivants sont inclus dans la vision applicative :

- document décrivant les composants logiciels ainsi que les flux de données entre ces composants ;
- document répertoriant les périmètres et niveaux de privilèges des utilisateurs et des administratreurs.

5.3 Vision de l'infrastructure technique

La vision de l'infrastructure technique doit illustrer d'une part le positionnement des dispositifs de contrôle d'accès physique ou de vidéoprotection au sein des différents sites, et d'autre part le cloisonnement des réseaux et les liens logiques entre eux. Les éléments suivants sont inclus dans la vision de l'infrastructure technique :

- schéma représentant les zones à surveiller et leur niveau de protection attendu ;
- schéma représentant les flux de circulation des individus ;

- schéma représentant le positionnement des dispositifs (têtes de lecture, UTL, caméras, systèmes de gestion, etc.) ;
- schéma représentant le cloisonnement physique et logique des réseaux, les plages d'adresses IP, les fonctions de routage et de filtrage ;
- document décrivant la liste complète des équipements physiques utilisés.

R30

Cartographier les systèmes de contrôle d'accès physique ou de vidéoprotection

Il est hautement recommandé de cartographier les systèmes de contrôle d'accès physique et de vidéoprotection. Cette cartographie doit contenir au minimum les éléments suivants :

- schéma représentant les zones à protéger/contrôler et leur niveau de protection attendu ;
- schéma représentant les flux de circulation des individus ;
- document décrivant la liste des acteurs ;
- document détaillant les processus organisationnels ;
- schéma représentant le positionnement des dispositifs (têtes de lecture, UTL, caméras, centres de gestion, etc.) ;
- schéma représentant le cloisonnement physique et logique des réseaux, les plages d'adresses IP, les fonctions de routage et de filtrage ;
- document décrivant la liste complète des équipements physiques utilisés ;
- document décrivant les composants logiciels ainsi que les flux de données entre ces composants ;
- document répertoriant les périmètres et niveaux de privilèges des utilisateurs et des administratreurs.

6
Sécurité des éléments support d'un système de contrôle d'accès physique

Les éléments support d'un système de contrôle d'accès correspondent aux éléments physiques du contrôle d'accès intervenant depuis la présentation du badge devant une tête de lecture jusqu'à l'ouverture de la porte. Une illustration de ces éléments support est proposée dans l'exemple d'architecture générale reproduit sur la figure 2.1 au début de ce document.

6.1 Badge sur support physique

Un badge ne doit contenir que les éléments strictement nécessaires aux phases d'identification et d'authentification, à savoir un identifiant (appelé UID) et un numéro d'identification dans le cas d'un badge à clé symétrique dérivée (cf. 9.1.2). Il est déconseillé d'y stocker d'autres informations. Toute information d'authentification mémorisée supplémentaire (ex. : mot de passe, code PIN), doit être stockée au niveau du GAC ou des UTL.

R31

Ne pas stocker d'informations critiques sur le badge

Les données relatives aux droits d'accès, aux périodes de validité et aux informations d'authentification autres que le numéro d'identification ne doivent pas être stockées dans le badge. Dès lors il est recommandé que ces informations soient stockées dans la base de données du GAC.

Information

Le traitement de données d'identification est soumis au cadre règlementaire RGPD entré en vigueur le 25 mai 2018. Les données biométriques sont qualifiées de « données sensibles » et leurs traitements doivent respecter les indications données dans le règlement type de la CNIL intitulé « Règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail »[22].

Les informations affichées sur le badge peuvent faciliter des actions malveillantes par les indications qu'elles peuvent fournir. Aussi, il est important de les minimiser (voir l'exemple de badge en figure 6.1).

22. Délibération de la CNIL n°2019-001 du 10 janvier 2019 [25].

R32

Minimiser les informations présentes sur les badges

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

- d'informations sur l'entreprise (nom, adresse)[23] ;
- d'informations sur le porteur (nom, prénom, poste), en dehors de sa photo ;
- les accès autorisés.

Un numéro de traçabilité peut être indiqué sur le badge à des fins administratives, mais ce numéro doit être différent du numéro d'identification. La photographie est tolérée car elle permet de vérifier rapidement que le badge appartient bien au porteur.

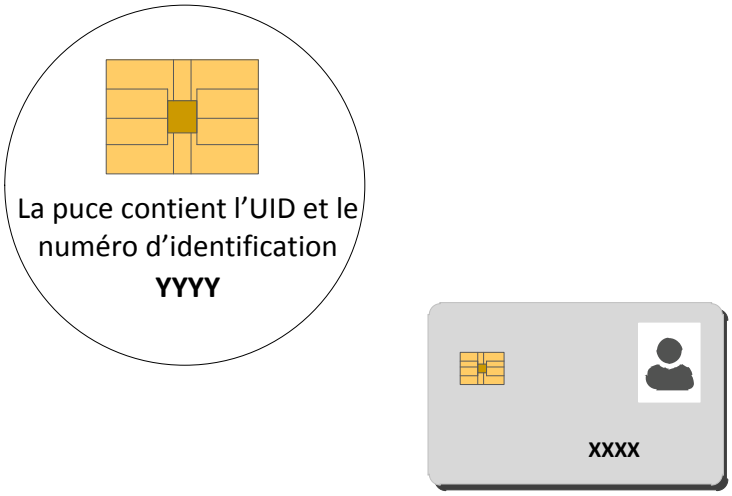

FIGURE 6.1 – Exemple de badge

Concernant les types de badges, les supports de type puce RFID[24], comparables aux antivols dans les magasins, ne permettent que l'identification, tandis que les supports de type carte à puce, comparables aux cartes de paiement bancaire, disposent de fonctions cryptographiques qui permettent une authentification.

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[25]. Il convient donc de s'orienter vers des produits récents, dont le niveau de sécurité est satisfaisant à date et dont le protocole de communication et la fonction anti-clone sont résistants à des attaques de niveau AVA_VAN.3[26].

23. Si des coordonnées sont indiquées sur le dos du badge pour faciliter sa restitution en cas de perte, elles ne doivent pas mentionner explicitement le nom de l'entité. Mieux vaut privilégier dans ce cas l'utilisation d'une boîte postale.
24. *Radio Frequency Identification*.
25. Attaque dans laquelle une transmission est frauduleusement répétée par une tierce partie interceptant les paquets sur la ligne.
26. Exigence d'assurance de sécurité des Critères Communs associée à l'identification de vulnérabilités pendant les phases de développement, configuration et exploitation.

R33

Privilégier l'utilisation de cartes d'accès certifiées avec un niveau de résistance aux attaques de niveau AVA_VAN.3

Dans la mesure du possible, il faut privilégier l'emploi de cartes d'accès intégrant un composant sous-jacent qui inclut la fonctionnalité de communication et qui a été certifié Critères Communs avec une résistance aux attaques de niveau AVA_VAN.3.

Un autre point important concerne l'unicité d'un badge. Certains badges ne sont pas garantis comme étant uniques. Il est possible dans ce cas d'être confronté à des doublons ce qui pose des problèmes de sécurité et des difficultés de gestion notamment pour leur traçabilité.

R34

Garantir l'unicité d'un badge

Un badge doit être garanti unique. Aucun doublon ne doit être possible sur le même système, ni sur un système existant dans l'entité ou hors de l'entité. Un badge doit pouvoir être réaffecté à une autre personne sans perte de traçabilité.

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. En effet, ces technologies demandent une grande maîtrise de la part des intégrateurs, notamment pour leur implémentation. Les chefs de projet et les acheteurs de systèmes de contrôle d'accès sont invités à s'inspirer des clauses proposées dans l'annexe D.1. Ils peuvent également s'adresser aux organisations professionnelles et au CNPP pour les orienter vers des intégrateurs, installateurs et mainteneurs certifiés.

6.2 Badge virtuel sur ordiphone

Un badge virtuel permet d'émuler sur un ordiphone la fonction d'un badge classique en s'appuyant sur des technologies telles que NFC [27] ou le *Bluetooth* basse énergie aussi appelé BLE [28]. Les avantages du badge virtuel tiennent dans l'absence d'une gestion de cartes physiques et dans le fait que l'ordiphone peut combiner l'authentification de l'utilisateur avec la fonction de badgeage (biométrie, code secret). Mais les inconvénients sont multiples :

- portée potentiellement importante du badge virtuel avec la technologie Bluetooth ;
  La technologie *Bluetooth* a une portée de plusieurs mètres. Cela peut s'avérer utile pour déclencher une porte de garage mais cela pose des problèmes pour l'ouverture d'un accès à des locaux :
  - risque de détection simultanée sur deux lecteurs qui sont proches,
  - gestion des cas où plusieurs personnes se présentent devant une tête de lecture.
- multiples usages possibles du NFC sur l'ordiphone ;
  La portée du NFC est de quelques centimètres, mais cette technologie peut être utilisée par plusieurs applications sur l'ordiphone (ex. : contrôle d'accès et application de paiement) ce qui nécessite de choisir l'application qui sera déclenchée en présence d'une tête de lecture.

27. *Near Field Communication*.
28. *Bluetooth Low Energy*.

- stockage sécurisé des clés et de l'identifiant chiffré sur l'ordiphone.
  Le stockage des secrets liés au contrôle d'accès sur un ordiphone n'apporte pas le même niveau de sécurité que le stockage de ces secrets sur une carte à puce recommandée pour le contrôle d'accès (certification Critères Communs avec une résistance aux attaques de niveau AVA_VAN.3).

R35

Éviter l'usage de badges virtuels sur ordiphone

Il est fortement déconseillé de recourir aux technologies de badges virtuels sur ordiphone qui n'offrent aucune garantie quant au stockage sécurisé des secrets liés au contrôle d'accès physique. De plus, la portée de la technologie *Bluetooth* n'est pas adaptée au contrôle d'accès de locaux, et les multiples usages possibles de la technologie NFC sur l'ordiphone apportent une complexité supplémentaire qui peut s'avérer très délicate à gérer.

6.3 Tête de lecture : protection des éléments chiffrés

Dans le cas des architectures où des 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 mécanismes de protection n'apportent pas une garantie suffisante pour parer à une attaque physique : pour la plupart des produits proposant ces fonctionnalités, il demeure possible d'accéder à l'intérieur de la tête par un espace 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 [29].

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 des lecteurs à façades standards ou anonymes (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 de ces opérations.

R36

Protéger les accès aux têtes de lecture

Les parties du système situées hors de la zone contrôlée, incluant les têtes de lecture, sont potentiellement des sources de vulnérabilités. Il est donc recommandé d'anonymiser les éléments apparents des têtes de lecture, et de contrôler minutieusement la liste des personnes habilitées à intervenir sur ces dispositifs.

Dans le cas des architectures où les têtes de lecture sont associées à un dispositif dédié à l'authentification du porteur (clavier ou lecteur biométrique), des informations sensibles sont échangées

29. Méthode propre au fournisseur du système de contrôle d'accès qui consiste à déployer les éléments secrets dans les dispositifs (UTL, têtes de lecture).

entre le dispositif et l'UTL (code secret, ou informations biométriques). Il convient de bien s'assurer que ces informations sont protégées en intégrité et confidentialité.

R37

Protéger les flux d'authentification du porteur entre le dispositif associé à la tête de lecture et l'UTL

Les informations liées au second facteur d'authentification, échangées entre le dispositif rattaché à la tête de lecture et l'UTL, doivent être protégées en intégrité et en confidentialité.

Il est nécessaire de se renseigner sur les caractéristiques techniques des têtes de lecture lors de l'achat et sur le paramétrage retenu lors de leur mise en œuvre. L'annexe D.2 contient la liste des exigences concernant les têtes de lecture, en relation avec le niveau de résistance logique attendu.

6.4 Unité de traitement local : accès physique réservé et Secure Access Module

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. Elle gère un groupe de têtes de lecture, chacune d'entre elles étant généralement associée à un ouvrant actionné par l'UTL.

L'UTL est un élément particulièrement sensible du système de contrôle d'accès. En effet, elle 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 configurations type, l'UTL détient aussi les éléments secrets cryptographiques permettant l'identification/l'authentification et la sécurisation de la communication avec le badge ou la tête de lecture. Enfin, l'UTL actionne les relais qui commandent l'ouverture des ouvrants.

R38

Protéger l'accès physique aux UTL

Il est fortement recommandé que les UTL soient situées à l'intérieur de la zone contrôlée dont elles commandent l'accès et ne soient pas accessibles facilement. Idéalement, elles doivent être à l'abri de tout accès frauduleux, dans un local technique fermé ou tout autre type d'emplacement sécurisé.

Les UTL sont parfois maintenues par des personnes tierces non habilitées à accéder aux clés cryptographiques. Cette situation devient préoccupante dans le cas d'une architecture où les UTL contiennent les éléments secrets et où les têtes de lecture sont transparentes (voir la configuration type n°1 décrite dans la section 6.5). Une solution consiste à utiliser des modules sécurisés de type « *Secure Access Module* [30] » (SAM) afin d'isoler et de protéger les éléments secrets au sein de l'UTL (voir également la section 9.1.2).

30. 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 clés cryptographiques en les isolant.

R39

Contrôler minutieusement les interventions effectuées sur les UTL

Il est impératif de disposer de la liste des personnes autorisées à accéder physiquement aux UTL et d'assurer également la surveillance des opérations effectuées sur ces équipements.

Les flux émis et reçus par les UTL supportent des données sensibles qu'il convient de protéger en intégrité et en confidentialité. Quel que soit l'emplacement de l'UTL (site local ou site distant), le chiffrement en intégrité et confidentialité des flux entrants et sortants des UTL est indispensable.

R40

Chiffrer et authentifier les flux émis et reçus par les UTL

Il est fortement recommandé que les communications entre les UTL ainsi que les communications entre les UTL et le centre de gestion soient protégées en intégrité et confidentialité, et que le mécanisme de chiffrement soit choisi et implémenté dans le respect des préconisations mentionnées dans le référentiel général de sécurité (RGS) [17] publié par l'ANSSI.

Il est nécessaire de se renseigner lors de l'achat des UTL et lors de leur mise en œuvre. L'annexe D.3 contient la liste des exigences concernant les UTL, en relation avec le niveau de résistance logique attendu.

6.5 Configurations type entre têtes de lecture et UTL

Il existe différents types de configurations, faisant intervenir les trois dispositifs principaux : le badge, la tête de lecture, et l'UTL. Ces éléments interviennent à différents stades et avec des mécanismes de sécurité variables.

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

R41

Implémenter en priorité la configuration type n°1

La configuration type n°1 est hautement recommandée. Elle reporte néanmoins le risque de l'exploitation d'une vulnérabilité de la tête de lecture sur l'UTL. Ainsi, les mesures de protection concernant l'UTL requièrent une attention toute particulière, notamment pour la protection des clés cryptographiques (voir la recommandation R38).
L'implémentation de la configuration type n°2 est déconseillée car la tête de lecture, située en zone non contrôlée, renferme des éléments secrets. Cette implémentation ne peut donc s'envisager que si la tête de lecture a fait l'objet d'une étude de sécurité approfondie.
Les configurations type n°3 et n°4 sont à proscrire car dans un cas le badge peut être cloné, et dans l'autre cas la liaison filaire n'est pas protégée.

Les schémas illustrant les quatre configurations type montrent la nature des flux véhiculés entre le badge et l'UTL, en passant par la tête de lecture. Le code de couleurs utilisé est le suivant :

- les flèches jaunes indiquent un flux chiffré entre le badge et l'UTL ou entre le badge et la tête de lecture ;
- les flèches bleues indiquent un flux chiffré entre la tête de lecture et l'UTL ;
- les flèches rouges indiquent un flux en clair.

6.5.1 Configuration type n°1, recommandée

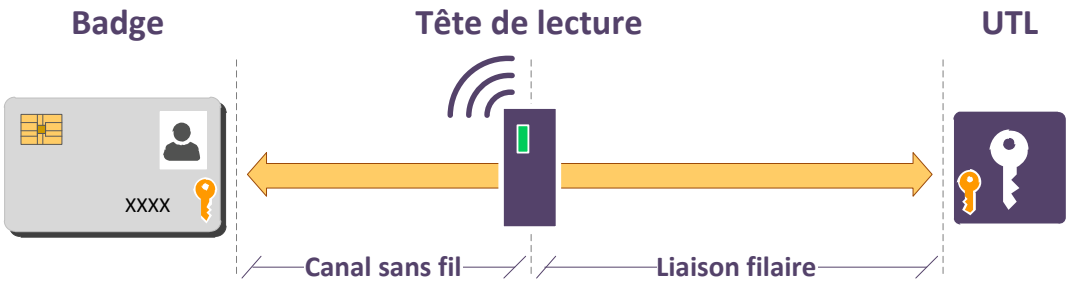

FIGURE 6.2 – Configuration type n°1 : tête de lecture transparente, authentification de bout en bout

Le badge, sécurisé [31], 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 :

- comme l'accès au numéro d'identification est protégé par chiffrement, 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 :

- comme l'UTL doit intégrer la capacité de gérer le protocole d'authentification, elle repose sur un équipement plus sophistiqué qui doit assumer la protection des clés cryptographiques.

31. Badges dont le protocole de communication et la fonction anti-clone sont certifiés Critères Communs avec un niveau de résistance aux attaques de niveau AVA_VAN.3 conformément à la recommandation R33.

6.5.2 Configuration type n°2, déconseillée

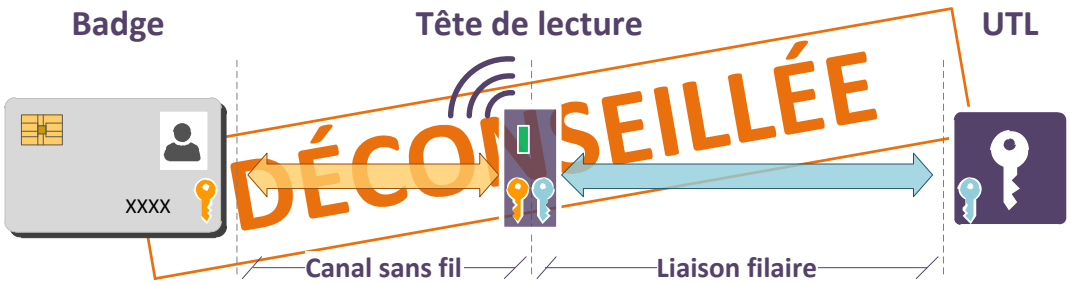

FIGURE 6.3 – Configuration type n°2 : tête de lecture intelligente, double authentification en coupure

Le badge, sécurisé [31], s'identifie et s'authentifie à la tête de lecture. Cette dernière a également une liaison sécurisée (avec authentification et intégrité) avec l'UTL. Elle envoie le numéro d'identification lu sur le badge à l'UTL.

Avantages :

- comme l'accès au numéro d'identification est protégé par chiffrement, 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.

Inconvénients :

- les éléments secrets permettant l'authentification de la carte ainsi que les éléments secrets permettant la protection de la liaison filaire se situent dans la tête de lecture, qui se trouve hors de la zone contrôlée ;
- 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.

6.5.3 Configuration type n°3, à proscrire

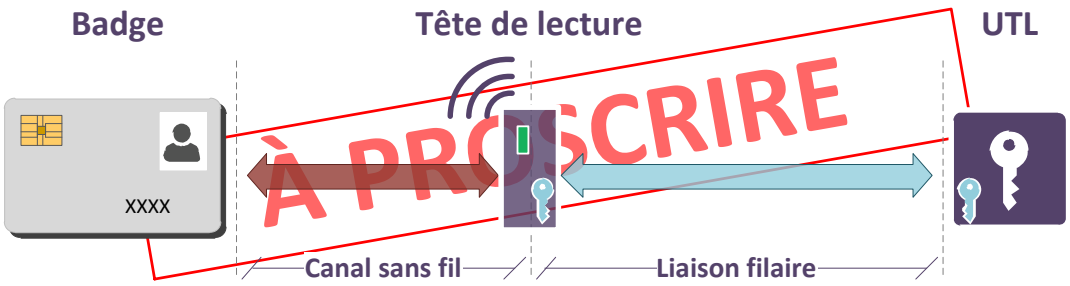

FIGURE 6.4 – Configuration type n°3 : Badge non sécurisé, avec chiffrement filaire seulement

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 :

- aucune information ne circule en clair sur la liaison filaire.

Inconvénients :

- comme l'accès au numéro d'identification n'est pas protégé par chiffrement, le badge peut être cloné. Le badge peut être identifié, mais pas authentifié ;
- les éléments secrets permettant la protection de la liaison filaire se situent dans la tête de lecture, qui se trouve hors de la zone contrôlée.

6.5.4 Configuration type n°4, à proscrire

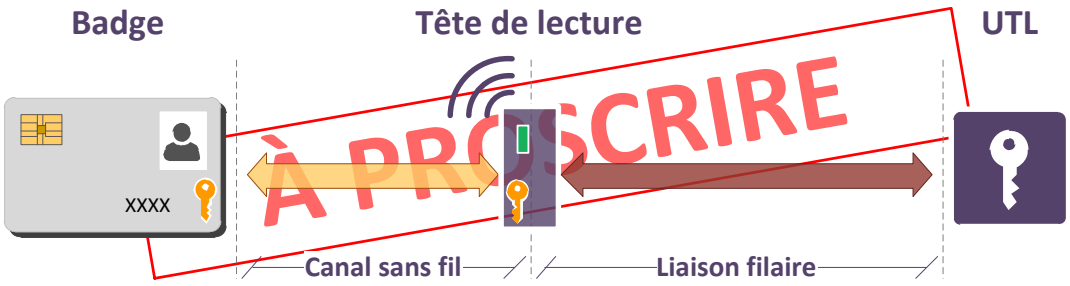

FIGURE 6.5 – Configuration type n°4 : Badge sécurisé, avec liaison filaire non chiffrée

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 :

- comme l'accès au numéro d'identification est protégé par chiffrement, 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 contrôlée.

6.6 Centre de gestion du système de contrôle d'accès

Le centre de gestion du contrôle d'accès physique regroupe un ensemble d'équipements qui doivent faire l'objet d'une vigilance permanente. Les serveurs de gestion du GAC manipulent des secrets et traitent d'informations personnelles sensibles. Les accès aux configurations de tous ces équipements doivent être sécurisés par l'application de mesures d'hygiène informatique (pare-feu, application régulière des correctifs de sécurité, antivirus, bonne gestion des comptes utilisateurs, authentification forte, etc.) [32].

Le respect d'une hygiène informatique stricte est d'autant plus crucial lorsque le système de contrôle d'accès est connecté à d'autres SI (voir le paragraphe 4.6).

R42

Sécuriser le GAC

Le centre de gestion du contrôle d'accès physique doit être considéré comme un SI à part entière. À ce titre, il est primordial de rappeler la nécessité de sécuriser l'ensemble des éléments constituant ce SI. Il est fortement recommandé d'appliquer strictement les règles d'hygiène informatique telles que décrites dans le guide de l'ANSSI consacré à ce sujet [5].

6.7 Logiciel de gestion du système de contrôle d'accès

Le logiciel installé sur le serveur de gestion [33] a pour rôle de communiquer d'un point de vue logique avec les UTL. C'est le point névralgique des systèmes de gestion d'accès physique. 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 consultation en temps réel et archivage sécurisé ;
- la remontée des événements au gestionnaire, que ce soit en temps réel sous la forme d'alertes lors de tentatives d'accès non autorisées ou de défectuosité d'un équipement, ou sous la forme de rapports journaliers par exemple ;
- la gestion des badges, des droits, des groupes, des dates d'expiration, etc. ;
- la sauvegarde régulière de la base de données ;

32. L'ANSSI publie de nombreuses recommandations sur son site : `http://www.ssi.gouv.fr/bonnes-pratiques`.
33. Le logiciel et le serveur de gestion du système peuvent être intégrés dans une « application matérielle » (*appliance*).

- le pilotage en temps réel de l'ensemble des UTL, en leur transmettant les éléments nécessaires au traitement local des demandes d'accès ;
- l'authentification pour contrôler l'accès au logiciel, et éventuellement la gestion de droits associée ;
- la gestion des alarmes en cas d'arrachement d'une tête de lecture.

7
Sécurité des éléments support d'un système de vidéoprotection

Les éléments support d'un système de vidéoprotection correspondent aux équipements physiques de vidéoprotection intervenant depuis la capture de l'image jusqu'à son traitement. Une illustration de ces éléments support est proposée dans l'exemple d'architecture générale reproduit sur la figure 2.1 au début de ce document.

7.1 Caméra

Les considérations de sécurité doivent intervenir dès le choix des caméras de vidéoprotection, ainsi que dans la configuration de ces dispositifs. Il est rappelé ici que les modèles récents de caméras IP s'apparentent très largement, en dépit d'un facteur de forme différent, à des ordinateurs classiques, aussi bien au niveau du matériel lui-même (micro-processeurs usuels, connectivité standard de type USB ou port série, etc.) que des composants logiciels qu'ils exécutent (système d'exploitation de type Linux, serveur Web ou console d'accès distant, etc.). À ce titre, les recommandations de sécurité portant sur ces équipements rejoignent largement celles qui s'appliquent aux matériels informatiques de type PC. On retiendra plus particulièrement les mesures suivantes :

- Les flux émis et reçus par les caméras doivent autant que possible être chiffrés et authentifiés, avec un protocole cryptographique interdisant le rejeu de flux. Cette mesure doit porter aussi bien sur les flux de remontée vidéo que sur les connexions d'administration distante des caméras. De nombreux modèles de caméras IP supportent des options de protection cryptographique des flux réseau, mais il est en général nécessaire de les activer spécifiquement dans la configuration des dispositifs. Il est par ailleurs souhaitable de privilégier dans ce cadre des protocoles cryptographiques génériques et éprouvés comme TLS ou IPsec, plutôt que des protocoles propriétaires spécifiques à un type d'équipement, dont il est difficile de vérifier la robustesse *a priori*. Le lecteur est par ailleurs invité à consulter les recommandations de l'annexe B1 du référentiel général de sécurité [19] pour le choix et le dimensionnement des mécanismes cryptographiques.

R43

Chiffrer et authentifier les flux émis et reçus par les caméras

Les flux émis et reçus par les caméras (images, administration) doivent être chiffrés et authentifiés par des protocoles tels que TLS ou IPsec.

- Il est courant que les caméras IP proposent une administration par port série, avec ou sans authentification. De telles interfaces trouvent toute leur utilité dans la configuration initiale des équipements. Or, il est en revanche nécessaire, au regard des possibilités d'accès physique

que pourrait avoir un attaquant, de les désactiver logiquement lors du déploiement effectif des caméras.

R44

Désactiver les interfaces locales d'administration des caméras

Il est fortement recommandé de désactiver les interfaces locales d'administration des caméras déployées, lorsque de telles interfaces existent.

- Le ou les mots de passe contrôlant l'accès aux fonctions d'administration sont généralement pré-positionnés à des valeurs par défaut lors de la fabrication des équipements.

R45

Remplacer les mots de passe par défaut des caméras

Les mots de passe par défaut des caméras doivent être remplacés par des mots de passe spécifiques, robustes et dans la mesure du possible différents pour chaque équipement. Des recommandations de sécurité relatives aux mots de passe sont décrites dans un guide de l'ANSSI consacré à ce sujet [1].

R46

Remplacer les certificats installés par défaut dans les équipements

Il est fortement recommandé de remplacer les certificats installés par défaut dans les équipements par des certificats générés par une infrastructure de gestion de clés maîtrisée par l'entité, et dédiée au système de vidéoprotection (cf. R53).

- Il est courant pour les équipements récents de proposer un ensemble de fonctionnalités avancées (par exemple réorientation de la caméra) dont la mise en œuvre n'est pas forcément nécessaire dans un cadre donné.

R47

Désactiver les fonctions d'administration non utilisées

De manière générale, il est recommandé de désactiver les fonctions qui ne sont pas réellement utilisées dans le cadre du déploiement considéré.

Il est souhaitable de prendre en compte ces recommandations dès la conception du système de vidéoprotection. La possibilité de réaliser les différentes opérations de configuration évoquées ci-dessus, en particulier la définition des mécanismes cryptographiques à mettre en œuvre, doit constituer un critère pour la sélection des modèles d'équipements à déployer. Au-delà de ces considérations, il convient de souligner qu'il n'est en général pas possible de juger *a priori* du niveau de robustesse des mécanismes de sécurité mis en œuvre au sein d'un équipement. Par conséquent, il est recommandé de faire mener une analyse indépendante de la sécurité des équipements sélectionnés, par exemple en entamant une démarche d'obtention d'un visa de sécurité ANSSI [34].

7.2 Caméra extérieure et boîtier de conversion analogique-numérique

Les caméras placées à l'extérieur de la zone contrôlée constituent des cibles de choix pour une personne mal-intentionnée. Au-delà du cloisonnement de la zone extérieure (voir le paragraphe 4.3.5),

34. Pour en savoir plus sur les visas de sécurité, se reporter à cette adresse : https://www.ssi.gouv.fr/visa-de-securite/.

l'emploi de technologies analogiques sur les caméras situées sur le réseau externe apporte une barrière supplémentaire par la rupture protocolaire entre le monde analogique et le monde numérique.

R48

Privilégier des caméras analogiques pour la vidéoprotection externe

L'emploi d'équipements différents au sein des réseaux de vidéoprotection internes et externes apporte une sécurité supplémentaire, en limitant les risques de voir une même vulnérabilité exploitée sur les deux réseaux. Il est recommandé de privilégier l'usage de technologies analogiques pour les caméras situées à l'extérieur de la zone contrôlée.

Les caméras extérieures sont alors connectées sur un boîtier de conversion analogique-numérique lui-même raccordé sur un réseau support dédié comme illustré sur la figure 4.3. Les boîtiers de conversion analogique-numérique sont utilisés pour convertir les signaux des caméras analogiques en signaux numériques IP à destination du centre de gestion (et *vice-versa*). Ces convertisseurs effectuent une rupture protocolaire ce qui apporte un niveau de sécurisation supplémentaire au regard de l'exposition des caméras extérieures. Cette sécurisation ne peut cependant être efficace que si les convertisseurs sont placés à l'intérieur de la zone contrôlée.

R49

Protéger l'accès physique aux boîtiers de conversion analogique-numérique

Il est fortement recommandé que les boîtiers de conversion analogiques-IP soient placés à l'intérieur de la zone contrôlée, à l'abri de tout accès frauduleux (à l'instar de la recommandation R38 sur l'emplacement des UTL).

7.3 Centre de gestion du système de vidéoprotection

Le centre de gestion du système de vidéoprotection, typiquement localisé au sein du poste de sécurité de l'entité concernée, est en général constitué d'un ensemble de serveurs qui réalisent la centralisation et le stockage des flux de vidéoprotection, permettent leur analyse et proposent des outils pour l'administration du parc de caméras. Élément central du système, ce centre de gestion est le seul (sous réserve de respect des recommandations d'architecture énoncées précédemment) à pouvoir communiquer avec l'ensemble des caméras. Il nécessite par conséquent une attention particulière en matière de sécurité. En plus des mesures classiques de sécurité physique, en particulier la localisation des équipements dans des locaux (ex. : poste de sécurité ou salle machines à accès restreint), les éléments du centre de gestion ne doivent pas être mutualisés avec le système d'information bureautique (au même titre que le reste du réseau fédérateur et du réseau support, voir *supra* R10) et doivent faire l'objet d'une application stricte des règles classiques d'hygiène informatique. On veillera ainsi plus particulièrement :

- à l'authentification individuelle des utilisateurs sur la base de mécanismes robustes ;
- à l'utilisation d'un réseau d'administration, si les équipements du centre de gestion sont administrés par le réseau ;
- à la mise en œuvre d'une politique adaptée de suivi des versions et de mise à jour des composants logiciels ;
- au strict contrôle des branchements de périphériques amovibles ;

- à la journalisation des opérations, notamment celles portant sur l'administration du parc de caméras et des serveurs de collecte des flux, et au contrôle régulier de ces journaux.

Il est par ailleurs souhaitable de faire vérifier le niveau de sécurité du centre de gestion par un audit réalisé par un prestataire d'audit qualifié PASSI [21].

R50

Sécuriser le SI de vidéoprotection

Le SI de vidéoprotection doit être considéré comme un SI à part entière. À ce titre, il est primordial de rappeler la nécessité de sécuriser l'ensemble des éléments constituant ce SI. Il est fortement recommandé d'appliquer strictement les règles classiques d'hygiène informatique telles que décrites dans le guide de l'ANSSI consacré à ce sujet [5].

8
Autres éléments de sécurité autour des SI de contrôle d'accès et de vidéoprotection

8.1 Horodatage

Les systèmes de contrôle d'accès physique et de vidéoprotection s'appuient chacun sur une source de temps pour horodater les événements générés par les dispositifs dépendant de ces systèmes. La cohérence des sources de temps utilisées par tous ces systèmes est cruciale, d'autant plus lorsque leurs informations sont croisées.

R51

Synchroniser les horloges des équipements sur une source de temps fiable

Il est fortement recommandé de synchroniser à l'aide du protocole NTP les horloges de tous les équipements qui composent les systèmes d'information de contrôle d'accès physique et de vidéoprotection depuis une source de temps fiable. Dans le cas où les informations issues d'un système de contrôle d'accès physique sont croisées avec celles d'autres systèmes de contrôle d'accès physique ou de vidéoprotection, les sources de temps de ces systèmes doivent être synchronisées.

8.2 Continuité de service

Il est nécessaire de mener 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 proportionnée afin de ne pas engendrer des coûts inutilement prohibitifs.

R52

Mener une réflexion sur le niveau de continuité de service souhaité

Il est fortement recommandé de mener une réflexion sur le niveau de continuité de service souhaité et réalisable d'un système de contrôle d'accès physique ou de vidéoprotection.

8.3 Problématique des signaux compromettants

Outre les menaces liées aux possibilités d'attaques physiques ou logiques, les équipements de vidéoprotection, comme tous les équipements électroniques, sont susceptibles de produire des rayon-

nements électromagnétiques parasites qui peuvent véhiculer des informations sensibles issues des traitements en cours sur l'équipement. En fonction de la sensibilité des locaux surveillés et de leur configuration géographique, ces problématiques de signaux compromettants doivent être prises en compte lors du déploiement de caméras intérieures, selon les modalités définies par la règlementation en vigueur [18]. Cette règlementation s'applique aux SI qui font l'objet d'une classification de défense [15], mais a valeur de recommandation pour les SI traitant d'informations sensibles non classifiées de défense.

8.4 Infrastructure de gestion de clés

Les protocoles tels que IPsec ou TLS, ainsi que le chiffrement des données vidéos archivées sur disque dur, reposent sur des clés cryptographiques de type asymétrique et nécessitent une solution assurant la création et la délivrance de certificats. Il en est de même pour les mécanismes d'authentification des badges qui s'appuient sur une cryptographie de type asymétrique. La gestion de ces certificats est facilitée par la mise en place d'une infrastructure de gestion de clés (IGC, aussi appelé PKI, *Public Key Infrastructure*). La mise en place d'une telle infrastructure doit néanmoins tenir compte des contraintes suivantes :

- gestion de plusieurs systèmes de contrôle d'accès ;
- gestion d'un système de contrôle d'accès et d'un système de vidéoprotection ;
- disponibilité des autorités de certification.

R53

Mettre en place une infrastructure de gestion de clés

La mise en place d'une ou plusieurs infrastructures de gestion de clés est recommandée, dans la mesure où cela facilite la gestion des certificats utilisés par les systèmes de contrôle d'accès physiques ou de vidéoprotection. Il est préconisé de dédier des sous-AC [35] pour chaque système dans le cas de mutualisation d'une infrastructure de gestion de clés entre un système de contrôle d'accès physique et un système de vidéoprotection. Cette recommandation s'applique également dans le cas de mutualisation d'une infrastructure de gestion de clés pour plusieurs systèmes de contrôle d'accès physique de sensibilité différente.

R54

Rendre accessibles les autorités de certification

Les autorités de certification de l'infrastructure de gestion de clés doivent être accessibles par tous les dispositifs utilisant des certificats délivrés par ces autorités, et ce quelle que soit la localisation de ces dispositifs.

35. Autorité de certification surbordonnée.

9
Principes cryptographiques appliqués au contrôle d'accès physique et à la vidéoprotection

Les mécanismes cryptographiques mis en œuvre au sein des systèmes de contrôle d'accès physique et de vidéoprotection concernent principalement les domaines suivants :

- authentification d'un badge de contrôle d'accès ;
- configuration des dispositifs de contrôle d'accès ;
- protection en authenticité et confidentialité des flux de contrôle d'accès et de vidéoprotection ;
- protection en confidentialité des vidéos sauvegardées sur disque dur.

Ce chapitre a pour objectif de donner les recommandations nécessaires à la mise en œuvre de ces mécanismes cryptographiques dans chacun des domaines pré-cités.

9.1 Cryptographie appliquée aux mécanismes d'authentification du badge

Les phases d'identification et d'authentification du badge s'effectuent via des mécanismes cryptographiques qui sont décrits dans cette section. Il est important de souligner que les badges sont particulièrement vulnérables aux techniques de clonage lorsque des mécanismes d'identification sont mis en œuvre sans être complétés par des mécanismes d'authentification. Acquérir des badges supportant l'authentification et disposant de mécanismes cryptographiques ne suffit toutefois pas en l'état. L'intégrateur doit activer correctement ces mécanismes lors de l'installation, sans quoi les badges ne sont utilisés qu'en identification, et sont donc susceptibles d'être clonés.

Les mécanismes cryptographiques doivent 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 B1 du référentiel général de sécurité (RGS) [19].

Les mécanismes cryptographiques d'authentification doivent être documentés. Il ne doit pas y avoir d'attaques connues permettant de cloner le badge, ou de rejouer une transaction. La taille des clés utilisées doit également être conforme au RGS.

R55

Vérifier la conformité des mécanismes cryptographiques aux règles décrites dans l'annexe B1 du RGS

Il est recommandé que la mise en œuvre des mécanismes cryptographiques appliqués aux mécanismes d'identification et d'authentification des badges soient conformes aux règles décrites dans l'annexe B1 du référentiel général de sécurité [19].

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

- une clé symétrique unique ;
- une clé symétrique dérivée d'une clé maîtresse ;
- une bi-clé asymétrique.

9.1.1 Clé symétrique unique

Une même clé secrète est employée par les badges et par les systèmes de contrôle [36]. Cette distribution à grande échelle présente un risque pour cette clé, qui peut être compromise par l'attaque matérielle d'un seul badge, ou du système de contrôle.

R56

Éviter les solutions reposant sur l'utilisation d'une clé symétrique unique

Dans la mesure du possible, il est hautement recommandé d'éviter les solutions de contrôle d'accès physique reposant uniquement sur une clé symétrique unique.

Il est cependant possible de déployer plusieurs clés symétriques sur ces systèmes de contrôle, ce qui permet de générer des familles de badges reposant sur des clés symétriques distinctes.

R56 -

Utiliser des clés différentes en fonction des types d'utilisateur

Dans le cas où l'installation d'une solution de contrôle d'accès physique reposant sur un mécanisme de clé symétrique unique est incontournable, il est fortement recommandé d'utiliser des clés symétriques distinctes en fonction du type d'utilisateur (salariés, visiteurs, etc.).

9.1.2 Clé symétrique dérivée d'une clé maîtresse

Chaque badge contient une clé unique, qui est dérivée par un mécanisme cryptographique à partir d'une clé maîtresse et d'un identifiant unique (UID) propre à chaque badge. L'UID est également contenu dans le badge. La clé maîtresse est donc présente dans la station d'enrôlement pour la création des badges, et dans le système de contrôle pour l'authentification des badges.

36. Le système de contrôle est le dispositif (UTL ou tête de lecture) permettant d'authentifier le badge.

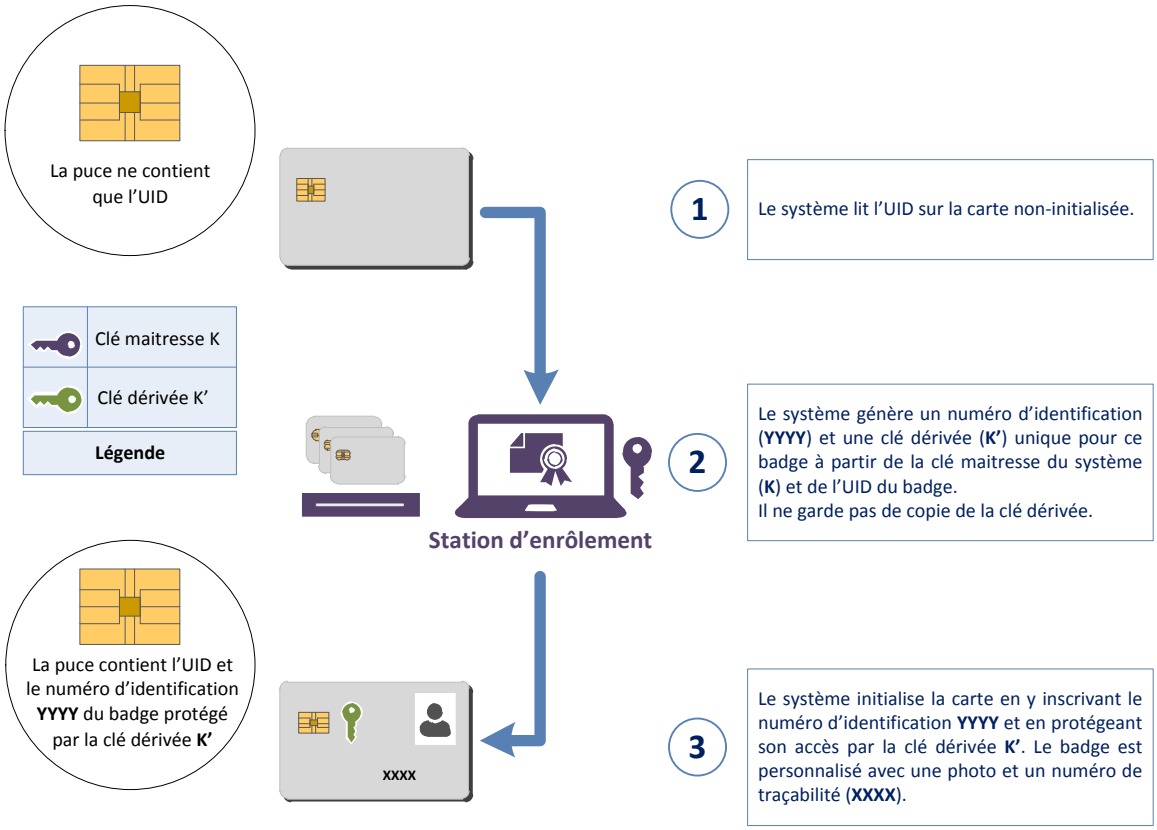

FIGURE 9.1 – Processus d'initialisation des badges à clé symétrique dérivée

Lors du contrôle, le système demande le numéro d'identification de la carte, puis, à partir de la clé maîtresse et de l'UID du badge, régénère la même clé dérivée, ce qui permet d'authentifier cette carte (voir le processus d'authentification d'un badge en annexe A).

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 la clé maîtresse, il est recommandé d'utiliser un module appelé *Secure Access Module* (SAM) : il s'agit d'une 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.

R57

Utiliser un module SAM

Dans le cas d'une utilisation de clés symétriques dérivées d'une clé maîtresse, il est hautement recommandé de recourir à l'utilisation d'un module *Secure Access Module* afin de protéger la clé maîtresse.

Lorsque plusieurs zones présentent des niveaux de protection attendus distincts (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 n'entraîne pas la compromission d'une zone de niveau de protection attendu plus élevé (voir l'illustration sur la figure 9.2).

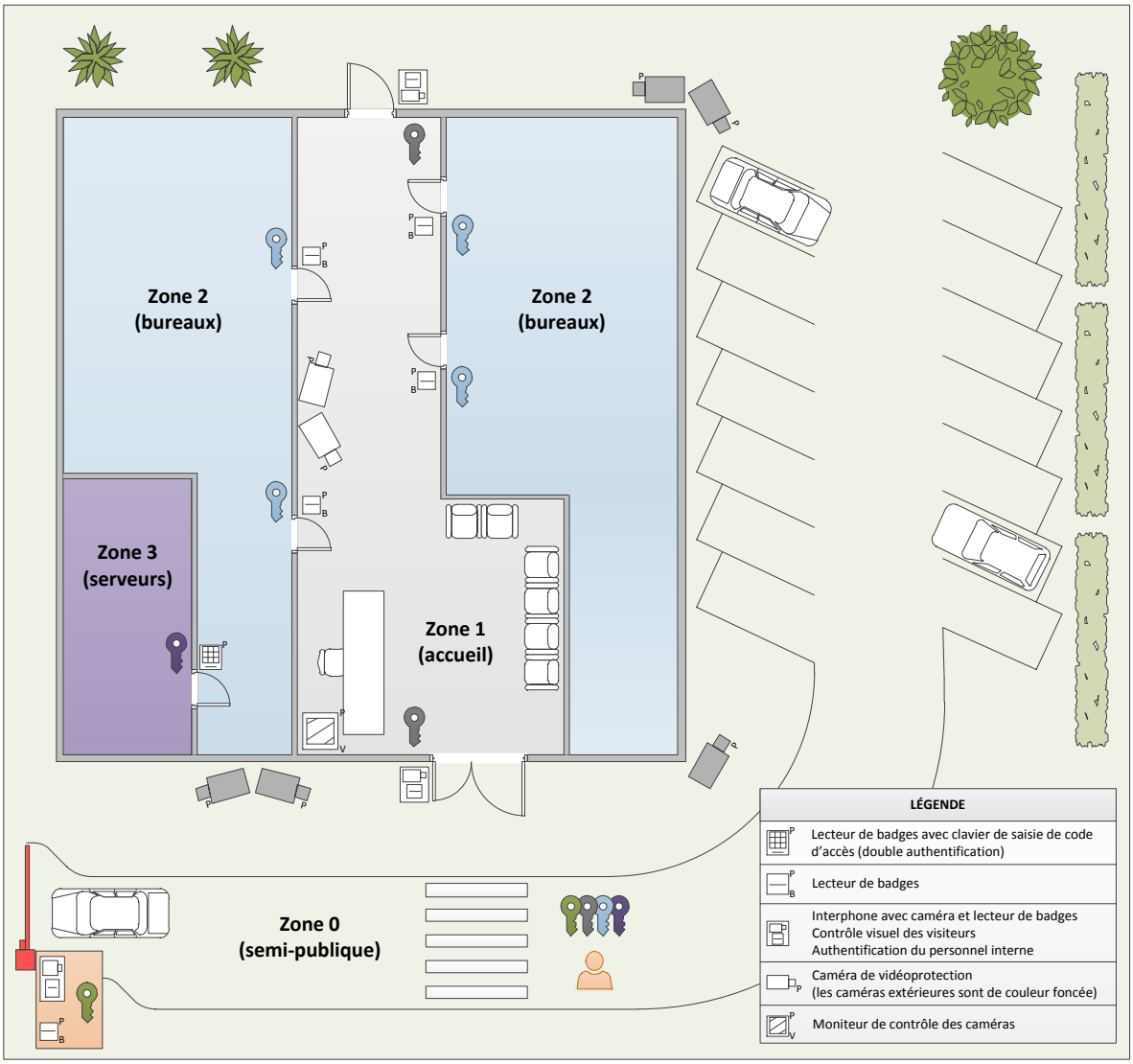

FIGURE 9.2 – Différenciation des clés utilisées selon le niveau de protection attendu des zones

R58

Privilégier la différentiation des clés maîtresses utilisées selon le niveau de protection attendu des zones

Il est recommandé de privilégier l'usage de clés maîtresses distinctes pour chaque niveau de protection attendu des zones.

9.1.3 Bi-clé asymétrique

Chaque badge et chaque système de contrôle possèdent leur propre clé privée. Lors de la phase d'authentification du badge, le système demande au badge de signer le message de réponse avec sa clé privée. La signature est vérifiée par le système de contrôle avec la clé publique du badge envoyée dans le message. Les messages envoyés par le badge sont chiffrés avec la clé publique du système de contrôle. Plus flexible, cette solution permet de mieux protéger les éléments les plus sensibles (les clés privées) en n'échangeant que des clés publiques et les certificats associés lors du contrôle.

Cette solution n'est toutefois pas encore très répandue car elle nécessite des cartes sans contact puissantes pour que le délai inhérent à la phase d'authentification ne soit pas prohibitif. Les atouts de cette solution plaident cependant pour son adoption car, en cas de compromission, de perte ou de vol d'un badge, seule la clé concernée devra être révoquée et changée et ce, contrairement aux solutions basées sur des clés symétriques (uniques ou dérivées). De plus, une attaque matérielle sur ce type de carte ne permettrait que de la cloner, sans qu'il soit possible d'en créer une différente. Cette solution présente enfin l'avantage de ne conserver aucun secret lié aux badges dans les UTL.

Cette solution nécessite la mise en place d'une infrastructure de gestion de clés (voir la section 8.4) en conformité avec l'annexe B2 du référentiel général de sécurité [16].

R59

Privilégier les solutions proposant un mécanisme d'authentification des badges reposant sur des bi-clés asymétriques

Bien qu'à la date de rédaction de ce guide, aucune solution de contrôle d'accès physique dotée d'un mécanisme d'authentification des badges reposant sur des bi-clés asymétriques n'ait été évaluée par l'ANSSI, il convient de privilégier ce type de solution plus flexible et plus sûr qu'une solution reposant sur des clés symétriques.

9.2 Cryptographie appliquée à la configuration des dispositifs de contrôle d'accès

En pratique, il s'avère souvent nécessaire d'employer d'autres clés cryptographiques dans le système de contrôle d'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).

Leur usage confère à ces clés une grande sensibilité. Cependant, n'étant pas nécessaires lors du contrôle (où seules les clés d'authentification sont utilisées), elles ne sont employées que lors de la création de badges par la station d'enrôlement, et lors de 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.

À noter qu'une vigilance particulière doit être portée sur la station d'enrôlement, dans la mesure où elle manipule régulièrement les clés d'écriture dans les cartes. Elle doit notamment être durcie et non connectée à Internet (voir la section dédiée aux postes d'administration 11.5).

La création, la gestion et le stockage de toutes les clés cryptographiques employées dans le système de contrôle d'accès physique sont des opérations essentielles pour la sécurité du système. Il convient d'être extrêmement vigilant lors de ces opérations afin d'assurer la protection des clés cryptographiques, qui sont le facteur principal de la sécurité du système.

R60

Protéger les clés cryptographiques employées dans le système de contrôle d'accès physique

Afin d'assurer la protection des clés cryptographiques employées dans le système de contrôle d'accès physique, il convient d'appliquer les recommandations du référentiel général de sécurité publié par l'ANSSI [16], notamment celles concernant la gestion des clés cryptographiques figurant dans l'annexe B2.

Une attention particulière doit être apportée à la méthode de mise à la clé du système de contrôle d'accès, notamment dans le cas déconseillé où les têtes de lecture renferment des clés (configuration type n°2 ; voir le paragraphe 6.5.2). Il ne doit pas être possible pour une personne extérieure (y compris le fournisseur ou le mainteneur du matériel) de changer les clés d'authentification sans que cela ne soit détecté.

R61

Détecter les changements de clés d'authentification

Il est fortement recommandé qu'un événement soit enregistré dans le GAC et qu'une alerte soit générée lors de tout changement de clés d'authentification.

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

R62

Anticiper la procédure de remplacement de clés cryptographiques en cas de compromission

La procédure de remplacement de clés cryptographiques en cas de compromission d'une clé doit être la plus transparente possible vis à vis des utilisateurs, et ne doit pas introduire de nouvelles failles de sécurité. Cette procédure doit être anticipée dès la phase de conception de l'architecture du système de contrôle d'accès physique et ce, quel que soit le type de clé utilisé.

9.3 Chiffrement et authentification des flux en provenance et à destination des dispositifs de vidéoprotection

Certaines solutions proposées par des constructeurs mettent en œuvre des mécanismes d'authentification et de chiffrement qui s'appuient sur des protocoles propriétaires. Or, dans la majorité

des cas, ces protocoles n'atteignent pas le niveau de maturité de protocoles d'authentification et de chiffrement éprouvés tels que TLS et IPsec. Il convient donc de bien choisir les dispositifs en fonction du niveau de maturité en sécurité numérique du constructeur et notamment des possibilités proposées dans ce domaine sur leur gamme de matériels de vidéoprotection.

R63

Privilégier les solutions d'authentification et de chiffrement non propriétaires

Il est fortement recommandé de privilégier les solutions s'appuyant sur des protocoles d'authentification et de chiffrement non propriétaires pour la sécurisation des flux entre les dispositifs et le centre de gestion.

9.4 Chiffrement des données vidéos sauvegardées sur disque dur

La confidentialité des données vidéos centralisées sur le VMS peut être assurée par leur chiffrement sur disque dur. Les mécanismes cryptographiques utilisés reposent sur des algorithmes de chiffrement et sur la création et la délivrance de certificats. Le choix de la solution de gestion vidéo doit tenir compte de la possibilité de mettre en œuvre le chiffrement des archives vidéos, ainsi que l'intégration possible de la solution dans une infrastructure de gestion de clés complètement maîtrisée.

R64

Privilégier les solutions de vidéoprotection proposant un bon niveau de maturité en matière de sécurité numérique

Il est fortement recommandé de privilégier des solutions de vidéoprotection proposant des protocoles standards pour le chiffrement des vidéos sauvegardées sur disque. La solution choisie doit également offrir la possibilité de s'intégrer dans une infrastructure de gestion de clés propre à l'entité (voir la section 8.4). Les algorithmes d'intégrité et de chiffrement mis en œuvre doivent respecter les préconisations mentionnées dans le référentiel général de sécurité (RGS) [17] publié par l'ANSSI.

10
Identification, authentification et gestion des droits d'accès pour une technologie sans contact

10.1 Identification

Dans un système reposant sur une technologie sans contact, l'identification est la présentation d'un badge à un lecteur. La communication de cette identité doit permettre d'attribuer de façon univoque à un utilisateur toute demande d'accès qu'il a effectuée.

R65

Associer un numéro d'identification unique à chaque utilisateur

Afin de permettre d'identifier de façon univoque toute demande d'accès, un numéro d'identification unique contenu dans un badge doit être associé à chaque utilisateur.

10.2 Authentification

Deux types d'authentification peuvent intervenir dans un système de contrôle d'accès : l'authentification du badge et l'authentification du porteur du badge.

- 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 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'un badge et de transmission sécurisée du numéro d'identification est présenté en annexe A.
- 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 [37] sélectionné parmi ce que l'on est (ex. : usage de la biométrie) et ce que l'on sait (ex. : saisie d'un mot de passe que seul le détenteur légitime du badge connaît).

37. Le badge constitue le premier élément : ce que l'on a.

R66

Privilégier des solutions de contrôle d'accès proposant à la fois l'authentification du badge et l'authentification du porteur

Dans la mesure du possible, il est recommandé de privilégier les solutions de contrôle d'accès physique proposant à la fois l'authentification du badge et l'authentification du porteur. L'activation de cette double authentification doit être étudiée en fonction du niveau de protection attendu associé à la zone contrôlée.

10.3 Biométrie

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

R67

Opter pour une authentification du porteur reposant sur un mot de passe

Dans la mesure du possible, il est recommandé de privilégier une solution de contrôle d'accès physique proposant une authentification du porteur par mot de passe. En effet, le mot de passe peut être gardé secret, être modifié, et il est surtout révocable.

R67 -

Opter pour une authentification du porteur reposant sur la biométrie

L'utilisation de la biométrie pour authentifier le porteur de badge dans une solution de contrôle d'accès physique est acceptable dans la mesure où les vulnérabilités de cette solution sont bien prises en compte (stockage des éléments biométriques sur le badge, révocation entrainant l'impossibilité pour le porteur de se voir affecter un nouveau badge avec les mêmes éléments biométriques).

10.4 Gestion des droits d'accès

10.4.1 Accès des utilisateurs permanents

Les utilisateurs permanents regroupent les collaborateurs de l'entité, ainsi que les prestataires.

10.4.1.1 Les collaborateurs

Les demandes liées aux badges servant au contrôle d'accès doivent être intégrées au processus de gestion des ressources humaines, lors de l'arrivée d'un collaborateur ou lors de son changement d'affectation. Les droits spécifiques (par exemple : accès à la salle serveurs) éventuellement demandés devraient être accordés, confirmés ou supprimés par les responsables de validation.

La création (programmation) et la remise d'un badge au porteur 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 d'accès, la création et la remise du badge doivent être effectuées sous le contrôle d'un opérateur du centre de gestion. Dans le cas d'une gestion centralisée du contrôle d'accès, la création et la personnalisation des badges doivent se faire selon un processus connu de l'opérateur du centre de gestion.

Lorsque la durée du contrat est connue à l'avance (stage, contrat à durée déterminée, etc.), la date de fin de validité du badge doit être programmée en conséquence. Le cas des contrats à durée indéterminée est plus délicat à gérer dans la mesure où la date de fin de validité n'est pas connue à l'avance. Il est toutefois fortement déconseillé de mettre en service des badges sans limitation de durée de validité. Aussi, une date de fin de validité d'un badge associé à un contrat à durée indéterminée doit être programmée.

R68

Programmer une date de fin de validité sur les badges de tous les collaborateurs

Il est fortement recommandé de programmer une date de fin de validité dès la délivrance d'un badge à un collaborateur. Dans le cas d'un contrat à durée indéterminée, une date de fin de validité du badge correspondant à une durée maximum de trois ans devra être définie, programmée et renouvelée à échéance.

Le changement d'affectation d'un collaborateur, intégré aux procesus de gestion des ressources humaines, doit entrainer une vérification de la pertinence des droits d'accès attribués à son badge. La restitution du badge doit aussi être intégrée aux processus de gestion des ressources humaines, lors du départ d'un collaborateur. Dans ce cas, les droits doivent être révoqués au plus tôt.

L'historique des accès doit être consultable. Une vérification régulière des accès utilisateurs doit être effectuée par les opérateurs du centre de gestion.

R69

Intégrer la gestion des badges des collaborateurs dans le processus de gestion des ressources humaines

Il est fortement recommandé que la gestion des badges (création, restitution) s'intègre dans le processus de gestion des ressources humaines, notamment dans les circuits d'arrivée et de départ. Les droits spécifiques du collaborateur doivent être accordés dans la mesure du possible par des responsables de validation ou par délégation à des responsables hiérarchiques, revus lors d'un changement d'affectation, et révoqués au plus tôt en cas de départ du collaborateur.

10.4.1.2 Les prestataires

La gestion de l'arrivée et du départ d'un prestataire est souvent du ressort des responsables de site. Si cette gestion ne pose aucun problème lors de l'arrivée du prestataire, il n'en va pas de même lors de son départ où le badge peut ne pas être restitué et donc rester actif. Il est donc particulièrement important de limiter dans le temps le badge d'un prestataire et ce, dès sa création.

R70

Programmer une date de fin de validité sur les badges des prestataires

Il est fortement recommandé de programmer une date de fin de validité dès la délivrance d'un badge à un prestataire. Dans le cas d'une mission de longue durée, une date de fin de validité du badge correspondant à une durée maximum de un an devra être définie, programmée et renouvelée si nécessaire.

10.4.2 Accès des utilisateurs particuliers

Certains profils particuliers d'utilisateurs (sous-traitants, personnel de maintenance, visiteurs, etc.) doivent être traités différemment des utilisateurs permanents tout en garantissant 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 souvent 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 une zone contrôlée.

10.4.2.1 Les visiteurs

En l'absence de mécanisme de dérivation des clés d'authentification à partir d'une clé maîtresse (clé symétrique unique, cf. section 9.1.1), il est recommandé d'utiliser des clés de chiffrement différentes pour les badges visiteurs particulièrement dans les cas suivants :

- il existe des zones inaccessibles aux visiteurs ;
- l'entité est répartie sur plusieurs sites.

La durée de validité de ces badges devra être limitée au strict minimum.

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, des procédures doivent être définies.

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 leur badge dans un temps restreint sur un même point d'accès (fonction d'escorte).

R71

Définir les procédures d'entrée des visiteurs

Il est fortement recommandé que des procédures d'obtention d'un badge par un visiteur soient définies. Ces procédures devront notamment indiquer les éléments suivants :

- la durée de validité du badge ;
- la mise en œuvre éventuelle de la fonction d'escorte ;
- le personnel autorisé à faire entrer un visiteur.

10.4.2.2 Les utilisateurs privilégiés, ayant des droits importants

La possibilité d'accorder à des porteurs de 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.

R72

Limiter le nombre d'utilisateurs ayant des droits importants

Le nombre de porteurs de badge ayant des droits importants doit être réduit au strict nécessaire. Il est hautement recommandé que leur badge bénéficiant de droits importants demeure toujours à l'intérieur de l'enceinte protégée. Un second badge pourra leur être attribué pour leur permettre de pénétrer dans l'enceinte puis de récupérer le badge bénéficiant de droits plus importants.

10.4.3 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 limitée (24 heures maximum). Parallèlement, cela doit 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 révélerait une probable perte non déclarée du badge permanent.

R73

Définir une procédure en cas de perte ou de vol d'un badge

En cas de perte ou vol de son badge, le personnel concerné doit le signaler sans délai afin de faire invalider son badge. En cas d'oubli d'un badge, le personnel concerné doit le signaler sans délai afin d'invalider temporairement le badge oublié et se faire délivrer un badge d'accès provisoire.

10.4.4 Badge 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 l'application utilisée pour le contrôle d'accès, une seconde application pour s'authentifier sur le SI métier ou bureautique de l'entité. 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 cependant de bien analyser les solutions existantes pour limiter les risques, en cas de perte ou vol du badge notamment. La compromission d'un élément ne doit pas entraîner la compromission des autres.

R74

Cloisonner chaque usage au sein d'un badge multi-usages

Afin de limiter le risque de compromission d'un usage depuis un autre usage d'un même badge, il est recommandé l'emploi de cartes d'accès reposant sur une plateforme sous-jacente (ex. : Javacard) qui inclut la fonctionnalité de cloisonnement, certifiée Critères Communs avec une résistance aux attaques de niveau AVA_VAN.5.

11
Administration

Les recommandations émises dans ce chapitre concernent à la fois les systèmes de contrôle d'accès physique et les systèmes de vidéoprotection.

11.1 Administration technique et administration métier

Il y a lieu de bien différencier l'administration technique de l'administration métier.

Administration technique

L'administration technique d'un système de contrôle d'accès physique ou de vidéoprotection est du ressort de l'administrateur système qui dépend de la direction informatique (DSI). L'administration technique inclut les fonctions suivantes :

- l'administration des routeurs, pare-feux et commutateurs réseau ;
- l'administration des serveurs et des systèmes d'exploitation ;
- l'administration des mécanismes de sauvegarde ;
- l'intégration dans le réseau de nouveaux dispositifs de contrôle d'accès physique ou de vidéoprotection ;
- la maintenance en condition opérationnelle (MCO) et en condition de sécurité (MCS) des systèmes d'exploitation ;
- la maintenance en condition opérationnelle et en condition de sécurité du logiciel de gestion.

Administration métier

L'administration métier d'un système de contrôle d'accès physique ou de vidéoprotection est du ressort de l'administrateur applicatif, de l'opérateur du centre de gestion et de l'opérateur d'enrôlement. L'administration métier inclut les fonctions suivantes :

- la supervision au poste de sécurité (fonctions de déblocage d'une personne coincée, etc.) ;
- la création de badges, les opérations d'enrôlement ;
- la visualisation de vidéos sauvegardées ;
- le réglage des caméras ;
- l'intégration dans le logiciel de nouveaux dispositifs de contrôle d'accès physique ou de vidéoprotection.

11.2 Comptes d'administration technique et métier

Les comptes d'administration peuvent être répartis en deux catégories, les comptes d'administration technique et les comptes d'administration métier. Les comptes d'administration technique se retrouvent sur les systèmes d'exploitation des serveurs, des stations de gestion, et plus généralement sur tout dispositif reposant sur un système d'exploitation. Ils sont également présents sur les équipements réseau. Les comptes d'administration métier concernent les logiciels de gestion de système de contrôle d'accès physique et de vidéoprotection.

Comme indiqué dans le guide sur les recommandations relatives à l'administration sécurisée des SI [13], les identifiants et secrets associés aux comptes d'administration, qu'ils soient technique ou métier, font partie des premières cibles d'attaque informatique car ils disposent de privilèges élevés. Il convient donc d'être très vigilant sur la gestion de ces identifiants et de ces secrets, en adoptant au minimum les mesures ci-dessous et en choisissant des équipements qui autorisent leur mise en œuvre :

- réinitialisation des mots de passe des comptes natifs ;
- utilisation de comptes d'administration individuels en lieu et place des comptes génériques lorsque cela est possible ;
- journalisation des événements liés aux comptes d'administration.

R75

Sécuriser les comptes d'administration technique et métier

Les recommandations du guide « recommandations relatives à l'administration sécurisée des SI » [13] doivent être appliquées, particulièrement celles concernant les comptes d'administration (paragraphe 7.1) qu'ils soient technique ou métier.

11.3 Flux d'administration technique et métier

Les échanges entre la station de gestion et le serveur de gestion contiennent des données sensibles qu'il convient de protéger en particulier lorsque cette station est située sur le réseau de production. Le chiffrement et l'authentification des flux d'administration doivent être aussi appliqués aux échanges entre les dispositifs et le serveur de gestion, et entre le poste d'administration système et les équipements du centre de gestion.

R76

Chiffrer et authentifier les flux d'administration technique et métier

Tous les flux d'administration doivent être chiffrés et authentifiés. Cela concerne :

- les flux entre la station de gestion et les serveurs de gestion ;
- les flux entre les serveurs de gestion et les dispositifs administrés ;
- les flux entre les postes d'administration technique situés sur le réseau d'administration, et tous les équipements du centre de gestion.

11.4 Sécurisation des ressources d'administration technique

L'administration technique d'un système de contrôle d'accès physique ou de vidéoprotection est du ressort des équipes réseau de la DSI. Toutes les recommandations relatives à l'administration sécurisée des SI sont applicables dans ce contexte.

R77

Appliquer les recommandations relatives à l'administration sécurisée des SI pour l'administration technique

Il est fortement recommandé d'appliquer sur les éléments d'infrastructure et les postes d'administration technique, les recommandations décrites dans le guide de l'ANSSI « Recommandations relatives à l'administration sécurisée des SI » [13], incluant les particularités inhérentes à l'administration d'un SI déconnecté telles que décrites dans le chapitre 12 du guide.

Les tâches d'administration technique doivent être effectuées depuis un poste d'administration durci et dédié, placé au sein d'un réseau d'administration. Le niveau de sécurité optimal est obtenu en mettant en œuvre un réseau d'administration dédié à l'administration technique des serveurs de gestion du contrôle d'accès physique ou de vidéoprotection et à l'administration des équipements d'infrastructure. En effet, l'utilisation d'un réseau d'administration dédié permet de limiter les flux d'administration aux seuls équipements du SI de contrôle d'accès ou de vidéoprotection ce qui diminue la surface d'attaque du réseau d'administration.

R78

Mettre en place un réseau d'administration dédié à l'administration des équipements du centre de gestion

Il est recommandé d'administrer les équipements des centres de gestion de systèmes de contrôle d'accès ou de vidéoprotection depuis un réseau d'administration dédié à cet effet.

Il est néanmoins envisageable que le réseau d'administration technique d'une infrastructure de contrôle d'accès ou de vidéoprotection soit mutualisé avec le réseau d'administration du SI de l'entité. Même si dans ce cas les risques de compromission du SI d'administration sont accrus par le nombre d'équipements administrés et le nombre de flux autorisés, ce réseau apporte la garantie d'un cloisonnement fort avec tout autre réseau potentiellement connecté à Internet.

R78 -

Mutualiser les ressources d'administration avec le réseau d'administration du SI

Dans le cas où la mise en place d'un réseau d'administration dédié à l'administration des centres de gestion de systèmes de contrôle d'accès ou de vidéoprotection n'est pas envisageable, il est recommandé de placer les ressources d'administration de ces systèmes dans le réseau d'administration du SI de l'entité.

11.5 Sécurisation des ressources d'administration métier

L'administration métier s'effectue depuis un ou plusieurs postes dédiés à cette activité, interconnectés avec le serveur de gestion de contrôle d'accès physique ou de vidéoprotection. Ces postes sont nommés stations de gestion dans ce document.

Une des particularités de l'administration des dispositifs de contrôle d'accès physique ou de vidéoprotection concerne le chemin emprunté par les flux d'administration. Ce chemin est en effet commun aux flux de production [38]. Or les stations de gestion sont des équipements vulnérables qui, en étant placés sur le réseau de production, sont accessibles depuis tous les dispositifs situés sur les réseaux support. L'ANSSI dans son guide sur les recommandations relatives à l'administration sécurisée des SI [13] recommande de connecter les ressources d'administration sur un réseau physique dédié à cet usage. Il convient donc d'être très vigilant quant à cette particularité, le centre de gestion et les stations de gestion présents sur le réseau de production devenant des cibles de choix pour les attaquants. Toutes les mesures de sécurité doivent être appliquées sur ces équipements.

R79

Appliquer les mesures de sécurité sur les systèmes de gestion et les stations de gestion

Comme spécifié dans les recommandations R42 et R50, il est fortement recommandé d'appliquer sur les systèmes de gestion et stations de gestion, des mesures de sécurité et notamment les recommandations décrites dans le guide de l'ANSSI « La défense en profondeur appliquée aux SI » [6].

Trois principaux rôles peuvent être distingués au sein de l'administration métier avec des droits particuliers qui leur sont associés :

- l'administrateur applicatif ;
- l'opérateur du centre de gestion ;
- l'opérateur d'enrôlement.

Une amélioration notable du niveau de sécurité des ressources d'administration métier consiste à dissocier ces rôles et à les répartir sur des stations de gestion distinctes, chaque station étant pourvue d'un logiciel spécifique dont les fonctions proposées correspondent au rôle qui est supporté. Les mesures de sécurité appliquées sur les stations de gestion peuvent être renforcées sur celles qui concentrent les droits les plus importants (ex. : suppression de l'accès à Internet sur les stations d'enrôlement et les stations d'administration de l'application). Il est de plus possible de protéger physiquement chacune de ces stations de gestion au sein d'un réseau dédié et protégé par une fonction de filtrage, à l'image de la station d'enrôlement illustrée sur la figure 2.1.

38. Les flux de production correspondent aux informations temps-réel remontées par les dispositifs (information de badgeage, vidéos, etc.).

12
Maintenance et exploitation

12.1 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. Il est fortement souhaitable de faire appel à des intervenants certifiés dans leur domaine (contrôle d'accès physique ou vidéoprotection) [39], ayant suivi des formations ciblées sur les technologies de sûreté et sur la cybersécurité, labellisées SecNumEdu-FC [40], comme celles proposées par le CNPP.

12.2 Maintien en condition opérationnelle

La maintenance en condition opérationnelle couvre plusieurs aspects dont la maintenance préventive des dispositifs, la maintenance opérationnelle et la disponibilité des systèmes de gestion.

Concernant le premier point, certaines actions doivent être effectuées de manière régulière pour garantir la résilience du système. Ces actions concernent en particulier les systèmes de contrôle d'accès physique avec la vérification de la batterie de l'alimentation de secours de l'UTL.

R80

Vérifier régulièrement les batteries des UTL

Dans le cadre de la maintenance globale du système de contrôle d'accès physique, la batterie de l'alimentation de secours de l'UTL doit être vérifiée au moins une fois par an [41]. Le bon fonctionnement de cette alimentation de secours, présente dans chaque UTL, est un gage de résilience du système.

Afin de minimiser les délais d'intervention en cas de panne matérielle, il est essentiel de disposer de matériels de rechange. Cette remarque vise notamment les têtes de lecture des systèmes de contrôle d'accès physique, et les caméras des systèmes de vidéoprotection. Ces matériels de rechange doivent être entreposés dans des locaux sécurisés, dont l'accès n'est autorisé qu'aux personnes habilitées.

Les dispositifs en panne doivent faire l'objet d'une extrême attention, car ils sont susceptibles de contenir des éléments cryptographiques qui, tombés dans des mains malveillantes, peuvent compromettre tout ou partie du SI de contrôle d'accès physique ou de vidéoprotection.

39. Le CNPP propose un schéma de certification de services notamment dans les domaines du contrôle d'accès physique et de la vidéoprotection.
40. Formation continue en sécurité du numérique. https://www.ssi.gouv.fr/entreprise/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/.
41. Fréquence de vérification minimum mentionnée par le CNPP dans son référentiel APSAD D83 [28].

R81

Contrôler minutieusement les dispositifs en panne contenant des éléments cryptographiques avant réparation ou mise au rebut

Une attention particulière doit être portée sur les dispositifs en panne susceptibles de contenir des éléments cryptographiques. Il est recommandé, lorsque cela est possible, d'effacer voire de supprimer ces éléments cryptographiques avant envoi du dispositif pour réparation chez un prestataire. Lors d'une mise au rebut d'un dispositif, il faut s'assurer que ces éléments cryptographiques ne pourront pas être extraits. Dans le cas où ces éléments ne peuvent pas être effacés, il convient de procéder à la destruction physique du dispositif.

La disponibilité des systèmes de gestion repose en grande partie sur la fiabilité des sauvegardes. Celles-ci doivent être effectuées de manière récurrente mais également de manière ponctuelle avant le déploiement de correctifs, avant l'intégration de mises à jour fonctionnelles, et après le paramétrage de nouveaux dispositifs. Des tests de restauration doivent également être planifiés de manière régulière.

R82

Effectuer des sauvegardes régulières

Il est hautement recommandé que des sauvegardes des systèmes de gestion soient effectuées *a minima* hebdomadairement et journalièrement en cas d'usage intensif. Il est fortement recommandé que des tests de restauration associés soient menés régulièrement (au minimum une fois par an).

12.3 Maintien en condition de sécurité

Du fait de leur caractère *a priori* déconnectés ou isolés, les systèmes de contrôle d'accès ainsi que les systèmes de vidéoprotection sont rarement maintenus en condition de sécurité. Une fois installés, la priorité est souvent donnée à leur bon fonctionnement. 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 peuvent être exploitées.

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

Au minimum, les mainteneurs doivent :

- notifier la présence de vulnérabilités sur les produits dont ils ont la charge ;
- proposer la mise en place de mesures qui remédient à ces vulnérabilités et un plan de déploiement des correctifs 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 doivent 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.

R83

Assurer le maintien en condition de sécurité

Il est impératif d'assurer un maintien en condition de sécurité pour les systèmes de contrôle d'accès physique et de vidéoprotection, au même titre que pour tout autre système d'information.

12.4 Procédures d'exploitation particulières des systèmes de contrôle d'accès physique

12.4.1 En cas de fonctionnement dégradé

On définit le fonctionnement dégradé, dans le cadre de ce guide, comme le fonctionnement du système de manière partielle à la suite d'un dysfonctionnement complet ou partiel des éléments qui le composent. Plusieurs types d'événements peuvent se produire et entraîner un fonctionnement dégradé. Ces 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 (voir la section 12.2). 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 règlementation sur la sécurité des personnes (cf. Annexe E),
  - 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) sont non opérationnelles ;

- indisponibilité 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 doit 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 (voir la recommandation R82) ;

R84

Privilégier les UTL disposant d'une copie de la base des droits

Il est recommandé de privilégier les UTL disposant d'une copie de la base des droits afin d'accroître la résilience du système notamment en cas de panne sur le serveur ou logiciel de gestion du système de contrôle d'accès physique.

- 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 support du système de contrôle d'accès, la panne relève de l'incident grave (cf. 12.4.2).

12.4.2 En cas de crise ou d'incident grave

Dans le cadre de ce guide, tout incident rendant le système non opérationnel dans sa quasi-totalité est perçu comme une crise ou un incident grave. Parmi ces incidents, deux types doivent être distingués :

- 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, il est à considérer que :

  > des événements de sûreté ou de sécurité pourraient survenir pendant cette période. La sécurité des personnes doit, bien entendu, continuer d'être assurée. Notamment, 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 (clé 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 doit avoir prévu des procédures assurant la sécurité des zones concernées par d'autre moyens (de type rondes de sécurité).

12.4.3 En cas d'alerte incendie

La règlementation nationale impose que les issues et dégagements permettent une évacuation rapide en cas d'incendie [42]. 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 comment le

42. Articles R. 4216-1 et suivants du Code du travail.

contrôle d'accès peut être assuré dans un tel cas, par exemple grâce à des moyens humains ou vidéos.

R85

Anticiper le retour dans les locaux à l'issue d'une alerte incendie

Le responsable du site doit déterminer (et tester) à l'avance comment sera assuré 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).

12.5 Procédures d'exploitation particulières des systèmes de vidéoprotection

Les procédures particulières des systèmes de vidéoprotection s'appliquent dans le cas d'une panne d'un dispositif ou dans le cas d'une panne survenant sur le VMS.

12.5.1 Panne d'une caméra

Le gestionnaire du système de vidéoprotection doit veiller à disposer d'un contrat de maintenance ou d'une organisation de maintenance interne assurant le remplacement du dispositif défaillant. Pendant la panne, le gestionnaire pourra être amené à faire contrôler physiquement la zone concernée par un agent de surveillance.

12.5.2 Panne du serveur ou logiciel de gestion de vidéoprotection

Ce cas de figure entraîne l'absence totale de visibilité sur les zones couvertes par les dispositifs de vidéoprotection. Cette situation critique doit être anticipée par l'entité notamment par la présence de procédures spécifiques détaillant les mesures de sécurité à mettre en place dans un tel cas comme, le contrôle visuel des zones sensibles par des agents de surveillance ou, la récupération des logs des dispositifs.

12.6 Infogérance

Il convient de signaler les risques inhérents au recours éventuel à un prestataire pour intégrer et maintenir en local ou à distance une infrastructure de contrôle d'accès physique ou un parc de caméras de vidéoprotection. Cette pratique relativement courante est notamment susceptible, selon la nature du prestataire et du contrat qui le lie à son client, d'entraîner le transfert ou la duplication de l'ensemble des données du contrôle d'accès ou des flux des caméras en dehors du système d'information du client, voire en dehors du territoire national. La couverture de ces risques, lorsque le recours à une externalisation du service s'avère nécessaire, passe par le respect de bonnes pratiques organisationnelles et contractuelles, selon la démarche décrite dans le guide « Maîtriser les risques de l'infogérance – externalisation des systèmes d'information » [4] publié par l'ANSSI.

Information

À la date de rédaction de ce guide, un nouveau référentiel des prestataires d'administration et de maintenance sécurisées (PAMS) est en cours d'élaboration par l'ANSSI. Ce référentiel inclut un ensemble de recommandations liées à la sécurisation des interventions effectuées par des prestataires sur un SI de l'entité.

12.6.1 Infogérance reposant sur un service externalisé

Dans le contexte particulier d'un système de contrôle d'accès ou de vidéoprotection dont le centre de gestion serait hébergé chez un prestataire tiers (ce cas est abordé dans la section 4.5 consacrée à l'externalisation des services de gestion), il convient notamment de porter une attention particulière :

- à la localisation des données collectées par le prestataire, aux mesures de sécurité liées à leur stockage et, à l'absence de duplication et de communication de ces données à des tiers (y compris dans le cadre des procédures de maintenance des équipements de collecte) ;
- à l'éventuelle mutualisation des services de collecte ou d'administration entre les différents clients ;
- à l'interconnexion entre le système de contrôle d'accès ou de vidéoprotection et le site de l'infogéreur.

R86

Maîtriser les risques de l'infogérance

Dans le cas d'un recours à une externalisation de l'administration d'une solution de contrôle d'accès physique ou de vidéoprotection, il est recommandé de se conformer à la démarche décrite dans le guide « Maîtriser les risques de l'infogérance – externalisation des systèmes d'information » [4] publié par l'ANSSI, et de recourir à un prestataire qualifié (voir la recommandation R26-). Une attention particulière doit être portée sur la mise en place de l'interconnexion entre le système de contrôle d'accès ou de vidéoprotection et le site de l'infogéreur.

12.6.2 Infogérance reposant sur un service de télémaintenance

Dans le cas où l'infogéreur intervient à distance pour maintenir ou administrer des ressources locales d'un système de contrôle d'accès physique ou de vidéoprotection, il convient d'éviter de mettre en place une solution de télémaintenance, à savoir l'accès direct aux équipements locaux depuis Internet. L'usage de ce type d'accès s'accompagne de risques de compromission parfois extrêmement élevés, c'est pourquoi son usage est fortement déconseillé.

R87

Éviter de mettre en place une solution de télémaintenance

Il est fortement déconseillé de mettre en place une solution de télémaintenance sur les ressources locales d'un système de contrôle d'accès physique ou de vidéoprotection, cette pratique pouvant engendrer des risques de compromission extrêment élevés.

12.6.3 Infogérance reposant sur un service d'administration à distance

L'administration à distance des équipements de contrôle d'accès ou de vidéoprotection nécessite la mise en place d'une interconnexion entre le site de l'infogéreur et le réseau d'administration du système de contrôle d'accès ou de vidéoprotection. Cette interconnexion accroit la surface d'attaque du réseau d'administration local de l'entité. Aussi, des mesures de sécurisation de cette interconnexion associées à une plus forte maîtrise du ou des postes d'administration doivent être mises en œuvre.

R88

Sécuriser la mise en œuvre d'une administration à distance

La mise en œuvre de l'administration à distance d'une solution de contrôle d'accès physique ou de vidéoprotection doit respecter les règles décrites dans le chapitre 10 du guide « recommandations relatives à l'administration sécurisée des SI » [13].

13
Journalisation et gestion des alertes

Deux familles d'événements peuvent être distinguées dans une infrastructure de contrôle d'accès physique ou de vidéoprotection :

- les événements métier ;

  Ces événements sont liés aux déplacements des personnes et plus généralement aux fonctions métier intégrées dans les serveurs de gestion, mais également aux événements liés aux actions effectuées sur les dispositifs de contrôle d'accès ou de vidéoprotection (maintenance, tentative d'arrachement, etc.) ;

- les événements techniques liés à l'infrastructure de contrôle d'accès et de vidéoprotection.

  Ces événements sont issus des équipements d'infrastructure et des systèmes d'exploitation présents sur les serveurs et stations de gestion.

Les mécanismes de collecte de ces deux familles d'événements sont différents dans la mesure où la collecte d'événements métier est effectuée par le logiciel de gestion, tandis que la collecte d'événements techniques est généralement effectuée sur un serveur de journalisation centralisé au sein du SI de l'entité.

La collecte des événements techniques n'est pas présentée spécifiquement dans ce guide car elle relève d'une gestion courante de tout SI, cet aspect étant traité dans le guide de l'ANSSI « recommandations de sécurité pour la mise en œuvre d'un système de journalisation » [7], et dans la section 9.2 du guide « recommandations relatives à l'administration sécurisée des SI » [13].

La gestion des alertes métier est une fonction proposée par les logiciels de gestion.

13.1 Collecte des événements métier

La collecte et la centralisation des événements métier sont effectuées nativement par la plupart des logiciels de gestion des systèmes de contrôle d'accès physique et de vidéoprotection. Il convient toutefois de s'assurer que l'horodatage des événements générés par les dispositifs est homogène (voir la recommandation R51), et que le centre de gestion est en capacité de sauvegarder tous ces événements conformément à la règlementation applicable au contexte dans lequel les dispositifs ont été déployés. Cette remarque concerne particulièrement le cas où les systèmes de contrôle d'accès sont couplés aux systèmes de vidéoprotection.

Concernant les opérations d'administration sur les dispositifs de contrôle d'accès physique et de vidéoprotection, il est indispensable que les événements associés à ces opérations soient bien journalisés.

R89

Centraliser les journaux d'événements métier des dispositifs sur le centre de gestion

Il convient de s'assurer que les événements métier issus des dispositifs de contrôle d'accès physique ou de vidéoprotection sont bien collectés et remontés vers le centre de gestion correspondant.

13.2 Analyse des journaux d'événements métier

Dans le cas d'un système de contrôle d'accès physique, les journaux d'événements, centralisés de manière exhaustive par le logiciel de gestion, 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 ;
- la liste des accès forcés ;
- la liste des portes ouvertes trop longtemps (POTL) ;
- etc.

Sans ces vérifications régulières, l'usage d'un faux badge est très difficilement détectable.

R90

Surveiller régulièrement les rapports générés par le GAC

Une surveillance des accès et des différents rapports doit être effectuée très régulièrement afin de détecter rapidement les anomalies et les tentatives d'accès frauduleuses.

13.3 Définition d'alertes spécifiques

En parallèle de rapports réguliers sur la base des journaux d'événements métier, il est recommandé de configurer des alertes en temps réel qui peuvent être rapidement prises en compte par le gestionnaire du système.

Ces alertes doivent 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, caméra, alertes systèmes et applicatives du serveur de gestion) ;
- saturation de l'espace de sauvegarde des vidéos ;
- accès refusé à une zone sensible ;
- porte restée ouverte plus longtemps qu'un temps donné.

R91

Configurer des alertes en temps réel

Il est recommandé de configurer des alertes en temps réel pour tout événement d'un niveau de criticité important.

Annexe A
Processus d'authentification d'un badge

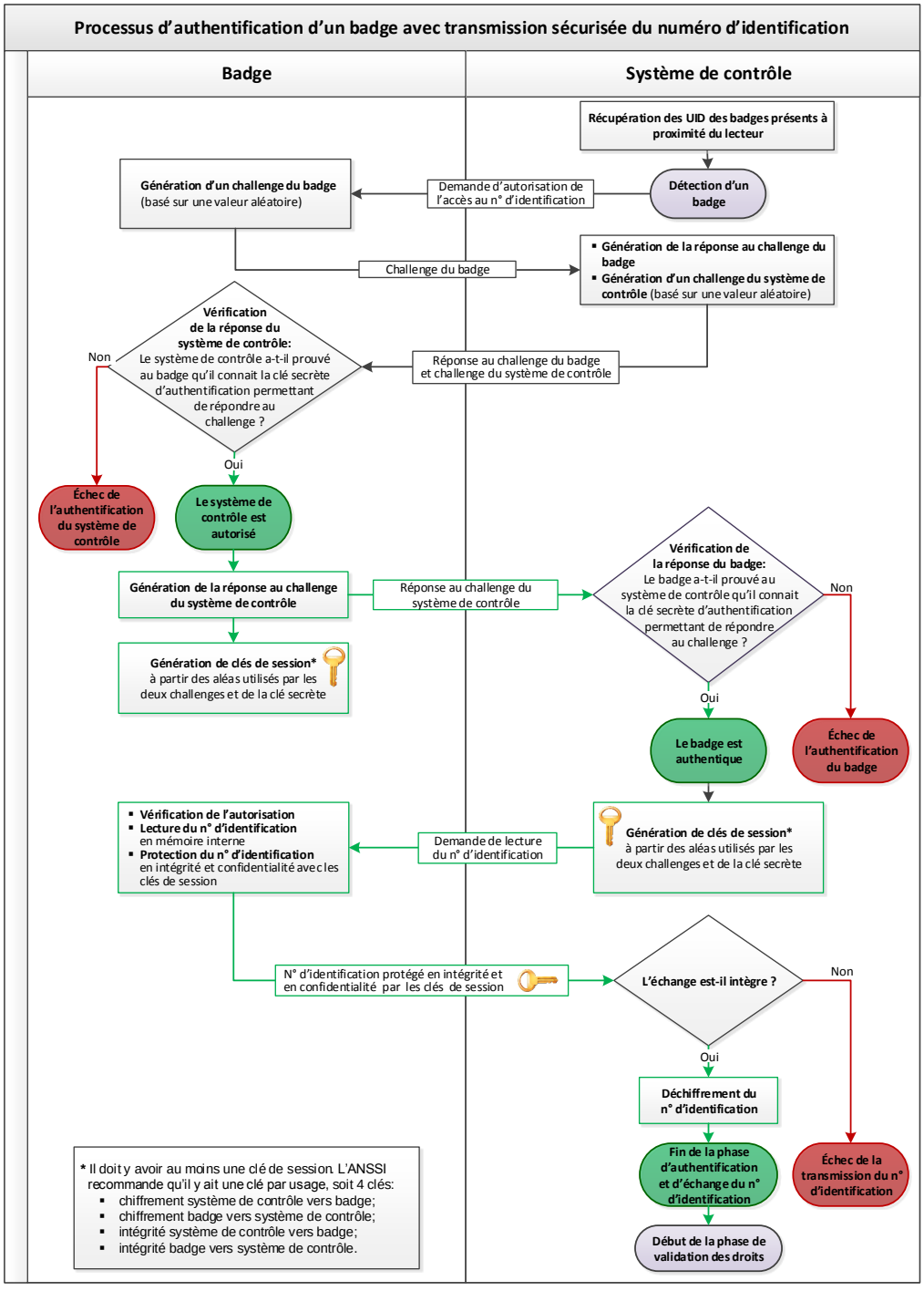

FIGURE A.1 – Authentification d'un badge et transmission sécurisée du numéro d'identification

(cf. section 10.2).

Annexe B
Exemple de processus organisationnel

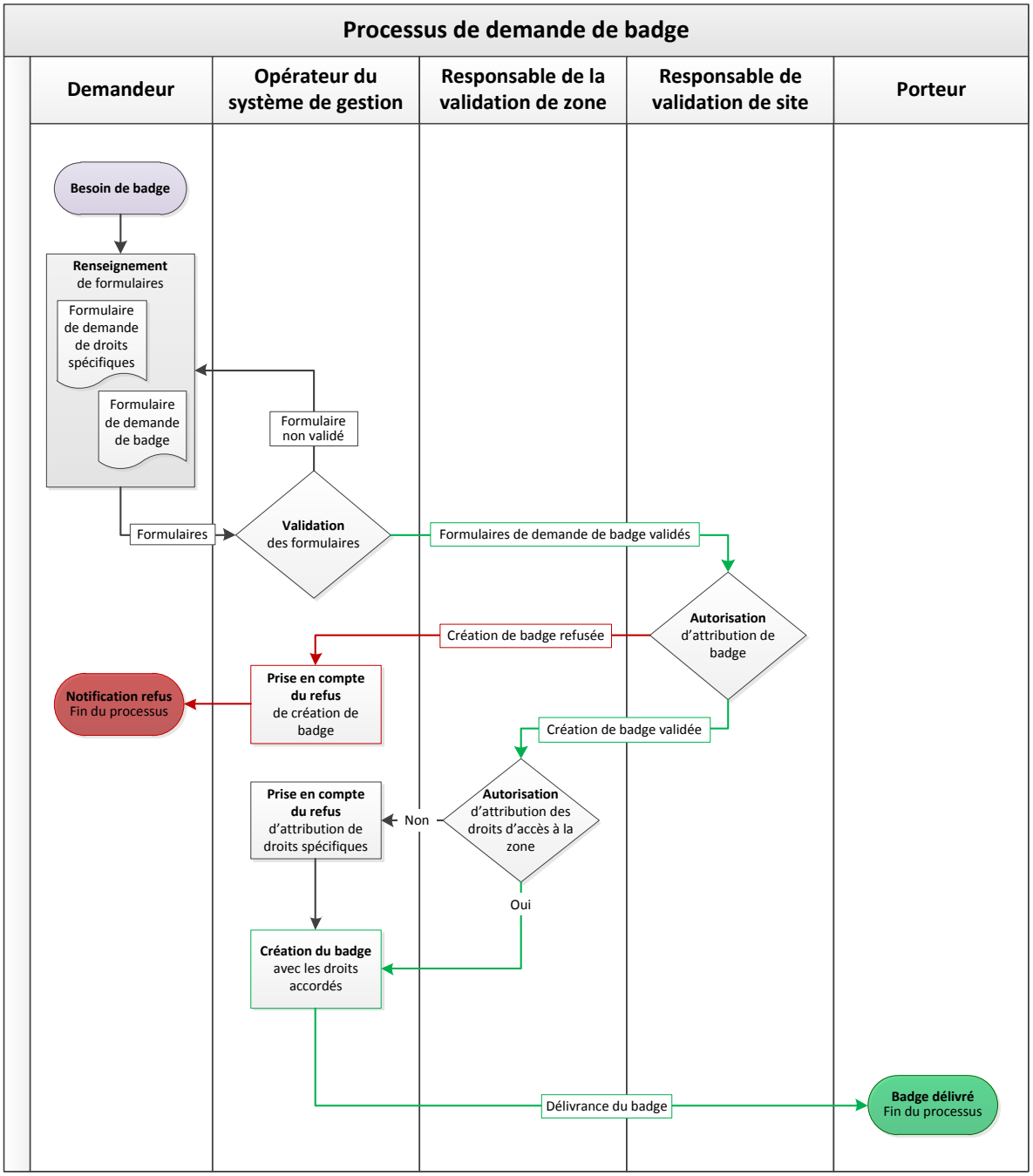

FIGURE B.1 – Exemple de processus organisationnel : demande de badge

(cf. section 3.7).

Annexe C
Exemple d'élaboration d'un schéma d'architecture

L'élaboration d'une architecture d'un système de contrôle d'accès et de vidéoprotection s'effectue au travers d'une démarche décrite dans le chapitre 4. L'objet de cette annexe est d'illustrer cette démarche par un exemple simple qui s'appuie sur les schémas proposés dans le chapitre 3 sur les étapes préliminaires à la mise en place d'un système de contrôle d'accès ou de vidéoprotection.

La figure C.1, synthèse des illustrations du chapitre 3, montre un exemple de découpage d'un site local en zones de différents niveaux de protection attendus. Quatre zones ont été définies depuis la zone 0, zone semi-publique et extérieure, à la zone 3, considérée comme la zone névralgique du site.

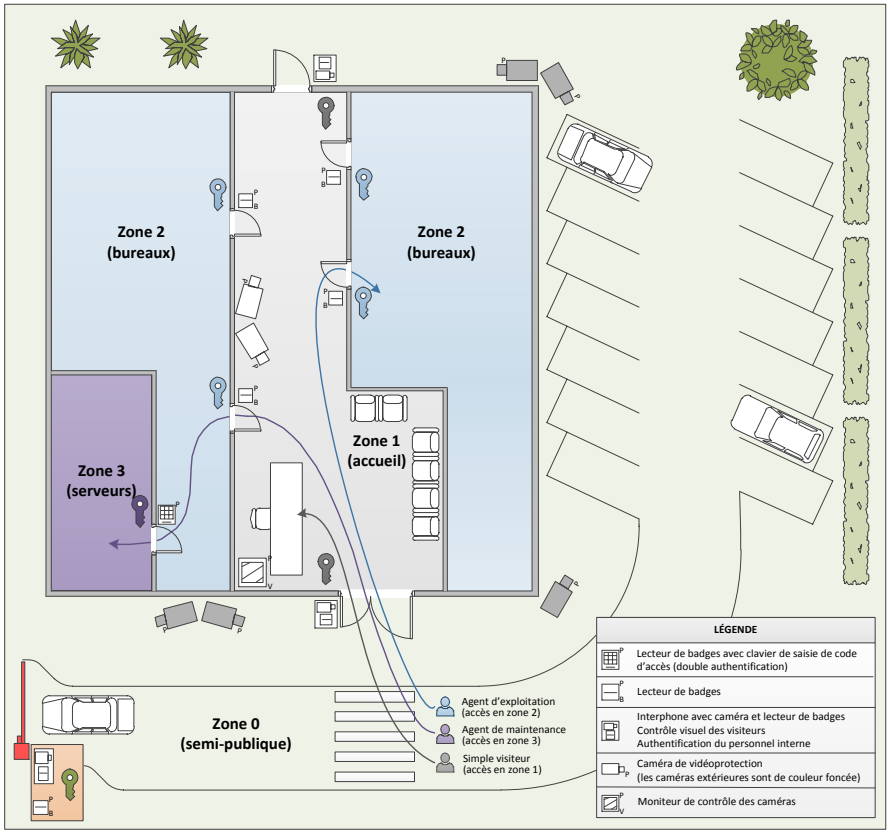

FIGURE C.1 – Découpage du site local en zones

L'analyse des flux de circulation des individus sur le site a permis de déterminer l'emplacement des dispositifs de contrôle d'accès et de vidéoprotection pour chaque zone comme l'illustre la figure C.1.

Nous supposerons en outre que la démarche préalable à l'élaboration du schéma d'architecture a acté les points suivants :

- sensibilité des zones ;

  Aucune zone à contrôler n'est soumise à une règlementation particulière par conséquent, la sensibilité des zones à contrôler est la même pour toutes les zones du site local.

- emplacement des centres de gestion ;

  Les centres de gestion du contrôle d'accès physique et de la vidéoprotection seront localisés sur un autre site que celui illustré sur la figure C.1.

- mutualisation de dispositifs issus de zones différentes ;

  L'analyse de risque prend en compte la mutualisation des dispositifs de contrôle d'accès liés aux zones 1 et 2 sur un même réseau support.

- informations sur le réseau fédérateur ;

  La liaison réseau existante entre le site à protéger et le site où sont situés les centres de gestion de contrôle d'accès et de vidéoprotection est partagée avec d'autres flux de l'entité, et transite par un réseau public.

- informations sur les interconnexions ;

  Deux interconnexions seront nécessaires sur le GAC : l'une concerne le système d'alertes, et l'autre concerne le système de détection d'intrusion.

- emplacement des stations d'enrôlement et des stations de gestion.

  Une station d'enrôlement sera installée sur le site local tandis que les stations de gestion des systèmes de contrôle d'accès et de vidéoprotection seront installées sur le site où sont localisés les centres de gestion.

À partir de ces éléments, en prenant en compte les règles de sécurité décrites dans le chapitre 4, et en les adaptant au contexte de cet exemple, nous pouvons énoncer les concepts suivants :

- un seul système de contrôle d'accès et un seul système de vidéoprotection seront mis en place ;
- les caméras extérieures situées en zone 0 seront de technologie analogique ;
- les réseaux support des caméras des zone 0 et 1 ne seront pas mutualisés ;
- chaque zone aura sa propre UTL ;
- les UTL affectées aux zones 1 et 2 seront mutualisées sur le même réseau support ;
- les UTL affectées aux zones 1 et 2 seront cloisonnées par VLAN sur le réseau support ;
- les réseaux support seront protégés par deux pare-feux, l'un pour le réseau de contrôle d'accès, l'autre pour le réseau de vidéoprotection ;
- les flux de contrôle d'accès seront acheminés vers le GAC au travers d'un tunnel IPsec ;
- les flux de vidéoprotection seront acheminés vers le VMS au travers d'un tunnel IPsec ;
- les centres de gestion seront protégés par des pare-feux ;

- une interconnexion devra être mise en place depuis le système de contrôle d'accès vers le système d'alertes ;
- une interconnexion devra être mise en place depuis le système de contrôle d'accès vers le système de détection d'intrusion ;
- une station d'enrôlement sera installée en zone 2 sur le site local.

L'ensemble de ces éléments ont conduit à l'élaboration du schéma d'architecture présenté en figure C.2.

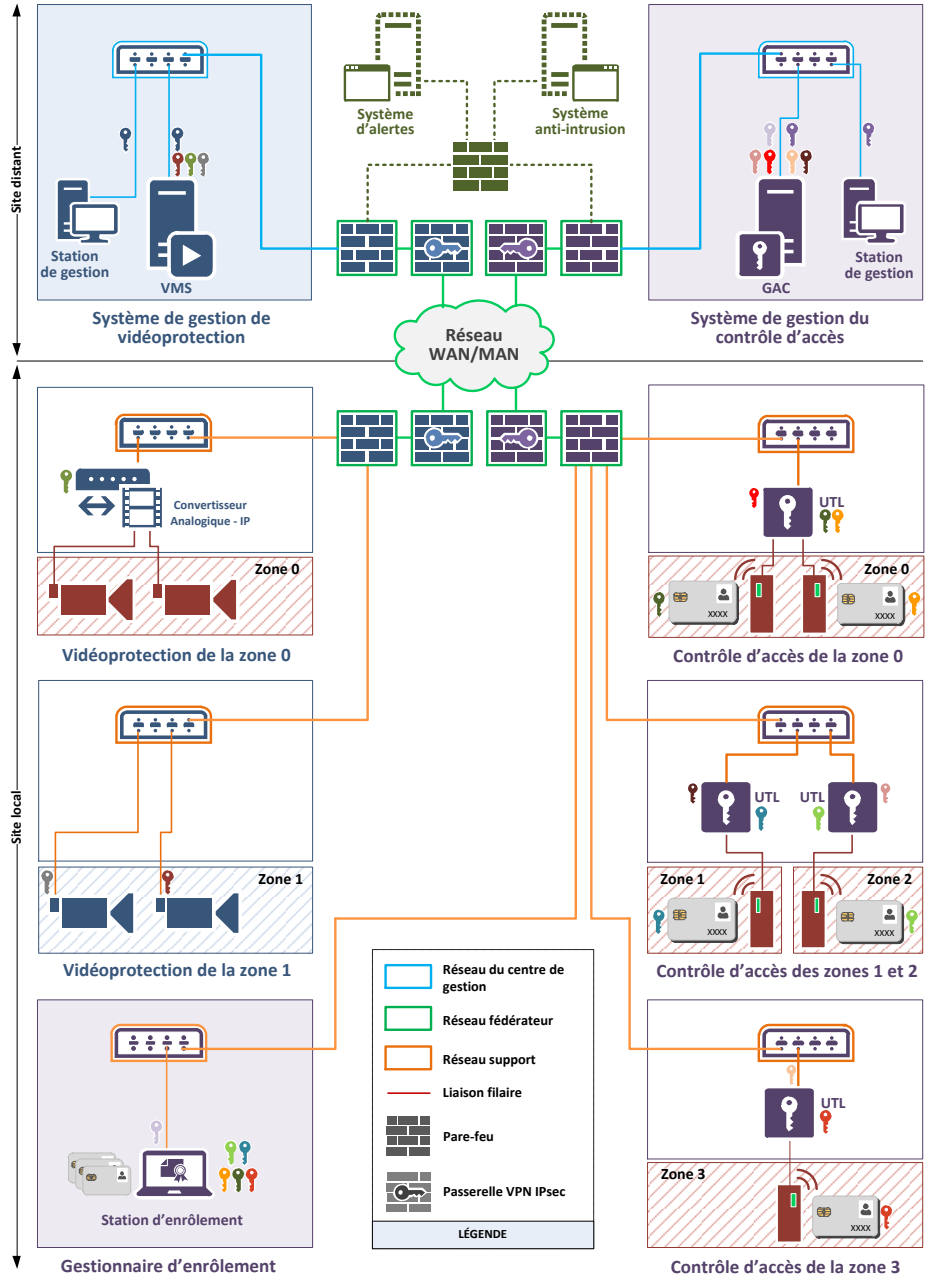

FIGURE C.2 – Schéma d'architecture

Sur cet exemple, les opérations d'administration des dispositifs et équipements du site local seront conduites selon les règles suivantes :

- l'administration technique des équipements réseaux du site local sera assurée par les équipes système depuis le réseau d'administration du SI de l'entité ;
- l'administration métier des dispositifs de contrôle d'accès et de vidéoprotection sera effectuée depuis les stations de gestion situées sur le site où sont localisés les centres de gestion.

Annexe D
Spécifications détaillées pour le cahier des charges d'un système de contrôle d'accès physique

Lors de la phase de préparation du cahier des charges en vue de la passation d'un marché ou d'un appel d'offres 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 dans cette annexe. Ces spécifications sont présentées selon quatorze grands thèmes correspondants aux différents éléments du système ou à son installation et sa maintenance :

- Badges ;
- Têtes de lecture ;
- UTL ;
- Réseaux et communications ;
- Performances ;
- Résilience ;
- Horodatage ;
- Contrôle d'accès ;
- Journalisation des événements et gestion des alarmes ;
- Stockage et archivage ;
- Biométrie ;
- Installation ;
- Administration métier et technique ;
- Maintenance.

Les exigences sont spécifiées par niveau de résistance aux attaques logiques. Ces niveaux de résistance (notés de L1 à L3) correspondent aux niveaux de sûreté définis de manière commune avec le CNPP (cf. section 3.4). La correspondance entre le niveau de sûreté et la résistance aux attaques logiques est détaillée dans le tableau D.1 qui indique également les méthodes d'authentification et les technologies de badge associées qui sont conseillées pour chaque niveau de résistance logique.

Niveaux de sûreté	Niveaux de résistance aux attaques logiques	Méthode d'authentification	Technologies
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.
II	L1	Authentification reposant sur une clé commune ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]).	Cartes ISO14443, authentification à cryptographie symétrique.
III	L2	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique.
IV	L3	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]) ; Authentification du porteur par un second facteur (information mémorisée ou élément biométrique).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique ; Saisie d'un code mémorisé ou d'un élément biométrique.

TABLE D.1 – Correspondance entre niveau de sûreté et niveau de résistance aux attaques logiques

Information

Dans un souci de lisibilité, les exigences sont formulées pour chaque niveau. Les exigences à appliquer pour atteindre un niveau de résistance aux attaques logiques spécifique comprennent les exigences de ce niveau et celles des niveaux inférieurs :

- pour atteindre le niveau de résistance aux attaques logiques L1, il faut appliquer toutes les exigences du niveau L1 ;
- pour atteindre le niveau de résistance aux attaques logiques L2, il faut appliquer toutes les exigences du niveau L1 et toutes celles du niveau L2 ;
- pour atteindre le niveau de résistance aux attaques logiques L3, il faut appliquer toutes les exigences du niveau L1, du niveau L2 et toutes celles du niveau L3.

43. Le protocole 3DES n'est pas recommandé par le RGS [17].

D.1 Badges

Résistance aux attaques logiques	Spécification
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 l'entité ou dans une entité tierce, et aucun doublon sur le même système).
L1	Le badge doit pouvoir être réaffecté à une autre personne, et ce, 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 visible 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 badge.
L2	Le protocole de communication et la fonction anti-clone du support de l'identifiant (badge, par exemple) doivent être certifiés selon les Critères Communs avec une résistance aux attaques de niveau AVA_VAN.3.
L3	Pas d'exigence spécifique pour ce niveau.

D.2 Têtes de lecture

Résistance aux attaques logiques	Spécification
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 doivent avoir fait l'objet d'une certification de sécurité de premier niveau (CSPN).
L2	Les têtes de lecture doivent comporter une signalisation visuelle d'accès autorisé et d'accès refusé, et doivent activer une signalisation sonore en cas de porte maintenue ouverte ou de porte forcée.
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 doit être doté d'une fonction « accès sous contraintes ».

D.3 UTL

Résistance aux attaques logiques	Spécification
L1	Les UTL analysent les droits du badge et délivrent l'ordre d'ouverture à la gâche ou à l'actionneur.
L1	Les UTL assurent la datation des événements et des alarmes.
L1	Les UTL transmettent les informations liées à la transaction, au serveur de gestion du système (GAC, UTS, ou autre équipement).
L1	Les UTL doivent émettre, vers le serveur de gestion du système, des informations sur les anomalies de fonctionnement qui leur sont propres et sur les anomalies des équipements qui leur sont associés.
L1	Les UTL s'auto-surveillent en générant des défauts internes. Ces alarmes sont 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 leur sont associés.
L1	La sécurisation des UTL doit 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 peuvent 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 la durée de coupure maximum retenue, 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 possèdent une mémoire (contenant les instructions du traitement) type EPROM [44] ou RAM [45] sauvegardée par batterie (24 heures minimum).
L2	Les UTL doivent être capables de gérer « l'anti *pass-back* » [46] des lecteurs qui lui sont associés.
L3	Pas d'exigence spécifique pour ce niveau.

44. *Erasable Programmable Read Only Memory*.
45. *Random Access Memory*.
46. Fonction qui évite qu'une personne entre deux fois dans une zone sans en être sortie au préalable.

D.4 Réseaux et communications

Résistance aux attaques logiques	Spécification
L1	Les cheminements de câbles sont 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 sont des liaisons dédiées au système de sécurité.
L1	Les liaisons filaires sont surveillées de manière à garantir qu'aucune tentative de fraude ne puisse être réalisée.
L1	La perte d'informations au niveau des liaisons doit être signalée et traitée comme une alarme.
L1	La fibre optique doit être privilégiée pour les liaisons entre bâtiments.
L2	La transmission des informations du système de contrôle d'accès se fait sur un réseau logique dédié à ce système.
L2	Les protocoles de communication utilisés (algorithmes de chiffrement inclus) doivent 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 doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]).
L2	La communication entre l'UTL et le serveur de gestion du système doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [19]).
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 sont 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 doivent 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.

D.5 Performances

Résistance aux attaques logiques	Spécification
L1	Le temps de réponse entre la présentation d'un badge et la réception de la commande d'ouverture de l'accès 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.

D.6 Résilience

Résistance aux attaques logiques	Spécification
L1	Au niveau du système et des équipements, une alimentation de secours d'une autonomie de X [47] heures minimum doit pallier une perte de l'énergie principale (batterie/onduleur).
L1	Le constructeur s'engage à fournir du matériel de remplacement identique ou interopérable pendant Y [48] ans.
L1	Tous les équipements sont dimensionnés 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.

D.7 Horodatage

Résistance aux attaques logiques	Spécification
L1	Toutes les données doivent être datées.
L1	La datation doit être précise à la seconde près et le système doit garantir la synchronisation de tous les équipements entre eux.
L1	La mise à l'heure locale au niveau serveur de gestion système doit être faite manuellement avec une possibilité de synchronisation externe par NTP [49].
L1	Le passage en heure d'été/heure d'hiver doit être automatique mais cette fonction peut être désactivée.
L2	Pas d'exigence spécifique pour ce niveau.
L3	Pas d'exigence spécifique pour ce niveau.

47. Le CNPP dans son référentiel APSAD D83 [28] indique une durée d'autonomie minimum de 120h.
48. Une durée de 12 ans minimum est conseillée.
49. *Network Time Protocol.*

D.8 Contrôle d'accès

Résistance aux attaques logiques	Spécification
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 seules les informations de début et fin doivent être enregistrées.
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 personnes présentes 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. Ex. : l'accès à la zone 2 sur la figure 3.1 n'est possible qu'après avoir badgé pour entrer dans la zone 1.
L3	Le logiciel doit posséder une fonction qui interdit l'accès à une zone, à une personne qui n'est pas sortie de la zone où elle était préalablement localisée (cette fonction ne s'applique qu'aux zones ayant un lecteur en entrée et en sortie).
L3	Le système 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 ».

D.9 Gestion des alarmes et événements

Résistance aux attaques logiques	Spécification
L1	La datation doit être effectuée au plus près de l'événement 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 niveau le plus faible.
L1	Une consigne spécifique doit pouvoir être attachée à chaque alarme. Cette consigne doit pouvoir 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, une alarme doit être générée si un porteur de badge tente d'accéder dans une zone intermédiaire sans avoir préalablement badgé en entrant dans les zones extérieures à cette zone.
L1	Les éléments secrets maîtres du système (clés cryptographiques) présents par défaut doivent être tous renouvelés automatiquement par le système et sauvegardés en lieu sûr par le responsable sécurité du site.
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) doivent être tous générés par un générateur aléatoire initialisé par une source d'entropie distincte du système et respectant les préconisations de l'annexe B1 du référentiel général de sécurité [19]. Ces éléments secrets doivent être saisis manuellement ou injectés par le responsable sécurité du site qui doit les sauvegarder en lieu sûr.
L3	Pas d'exigence spécifique pour ce niveau.

D.10 Stockage et archivage

Résistance aux attaques logiques	Spécification
L1	Le logiciel doit permettre d'effectuer des archivages et stockages avec identification précise des périodes correspondant aux données.
L1	Les données du système sont 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.

D.11 Biométrie

Résistance aux attaques logiques	Spécification
L1	L'identification biométrique est acceptable.
L2	La biométrie ne peut venir qu'en complément d'un badge.
L3	L'usage d'un code (révocable), en complément obligatoire du badge, est préférable à l'usage de la biométrie (non révocable).

D.12 Installation

Résistance aux attaques logiques	Spécification
L1	Pas d'exigence spécifique pour ce niveau.
L2	Le système doit être installé par du personnel certifié par un organisme habilité, dans la mesure où un schéma de certification adéquat existe [50]. Les certificats doivent être présentés au commanditaire.
L3	Pas d'exigence spécifique pour ce niveau.

D.13 Administration métier et technique

Résistance aux attaques logiques	Spécification
L1	L'administration technique doit être effectuée depuis un poste d'administration durci et dédié.
L1	Les flux d'administration technique et métier doivent être chiffrés et authentifiés.
L2	Pas d'exigence spécifique pour ce niveau.
L3	L'administration technique des équipements doit être effectuée depuis un réseau d'administration dédié.

50. Voir la section 12.1.

D.14 Maintenance

Résistance aux attaques logiques	Spécification
L1	L'usage de la télémaintenance doit être évité.
L2	La maintenance doit être assurée par du personnel certifié par un organisme habilité, dans la mesure où un schéma de certification adéquat existe [51]. Les certificats doivent être présentés au commanditaire.
L2	Les tiers de maintenance s'engagent à notifier la présence de vulnérabilités sur la version déployée des systèmes dont ils ont la responsabilité. A minima ils proposent les correctifs ou les mesures de contournement dans un délai fixé par le commanditaire après leur publication par l'éditeur. Idéalement ils s'engagent à déployer les patchs et correctifs de sécurité après la mise à disposition par les fabricants des équipements concernés.
L2	Un suivi des versions majeures déployées sur les différents systèmes doit être fourni régulièrement (périodicité à définir par le commanditaire). Ce suivi doit mettre en avant les différences entre les versions déployées et les versions compatibles avec le système les plus récentes.
L3	Pas d'exigence spécifique pour ce niveau.

51. Voir la section 12.1.

Annexe E
Contraintes règlementaires concernant le contrôle d'accès physique

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 au regard du règlement général sur la protection des données (RGPD), dans le cadre de la protection des données à caractère personnel, en fonction des dispositifs mis en place. Pour finir, des contraintes plus spécifiques peuvent s'appliquer en fonction des zones contrôlées.

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.

E.1 Protection des personnes

En cas de catastrophes nécessitant une évacuation (incendies, risques potentiels liés à l'environnement de travail, etc.), 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 personnes présentes à l'intérieur du bâtiment qui ouvrent une issue de secours. Cela montre bien l'importance d'un système particulièrement redondant pour garantir la plus grande résilience possible.

E.2 Traitement de données à caractère personnel

Depuis la date d'entrée en vigueur du RGPD (25 mai 2018), il n'existe plus de formalités préalables auprès de la CNIL, sauf cas très spécifiques relevant des articles 31 et 32 de la loi n° 78-17 du 6 janvier 1978 (loi Informatique et Libertés). L'entité doit toutefois s'assurer de la licéité des traitements de données à caractère personnel liés au système de contrôle d'accès. Deux cas se présentent, selon la nature des données à caractère personnel qui sont traitées :

- traitement de données à caractère personnel non biométriques ;
- traitement de données à caractère personnel biométriques.

E.2.1 Traitement de données à caractère personnel non biométriques

Dans le cas où aucune donnée biométrique n'est collectée ou enregistrée par le système de contrôle d'accès, l'entité doit engager les actions suivantes :

- informer et associer, dans la mise en œuvre du système de contrôle d'accès, le délégué à la protection des données (DPD[52]) ;
- inscrire les traitements de données dans le registre des activités de traitement tel que décrit dans l'article 30, chapitre IV du RGPD [26].

E.2.2 Traitement de données à caractère personnel biométriques

Si des données biométriques sont collectées ou enregistrées par le système de contrôle d'accès, il faut justifier la raison pour laquelle de telles données doivent être collectées par l'entité (car le RGPD considère qu'il s'agit de données sensibles dont le traitement est en principe interdit sauf justification particulière (cf. article 9)). L'entité doit alors engager les actions suivantes :

- respecter les exigences formulées dans la délibération de la CNIL n° 2019-001 du 10 janvier 2019 portant sur le règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail [25] ;
- conduire une analyse d'impact relative à la protection des données (AIPD) tel que décrit dans l'article 35, chapitre IV du RGPD [27]. Si cette étude fait apparaitre des risques résiduels trop importants sur les droits des personnes concernées, la CNIL devra être consultée ;
- informer et associer dans la mise en œuvre du système de contrôle d'accès le délégué à la protection des données (DPD) ;
- inscrire les traitements de données dans le registre des activités de traitement tel que décrit dans l'article 30, chapitre IV du RGPD [26].

Information

Dans le cas où le traitement est mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, le traitement doit être autorisé par décret en Conseil d'État après avis motivé et publié de la CNIL (cf. article 32 de

52. DPO en anglais : *Data protection officer*.

la loi Informatique et Libertés).

E.3 Implication des instances représentatives du personnel

La mise en place d'un système de contrôle d'accès implique un changement des conditions de travail. La direction doit donc informer et consulter les instances représentatives du personnel de son intention de mettre en place un contrôle d'accès physique.

E.4 Personnes à mobilité réduite

Lorsque les zones controlées sont susceptibles d'accueillir des personnes handicapées à mobilité réduite, il est important de prendre en compte la loi Handicap du 11 février 2005 relative à l'accessibilité des personnes à mobilité réduite, ainsi que ses décrets et arrêtés d'application en vigueur. Les têtes de lecture par exemple doivent être installées à une hauteur par rapport au sol de 0,90m à 1,30m par rapport au sol, ainsi que tout dispositif additionnel d'authentification (boitier de saisie de code PIN, d'empreinte biométrique, etc.).

E.5 Autres

Attention, certaines zones contrôlées sont concernées par des règlementations particulières qui impacteront les caractéristiques du système de contrôle d'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 règlementaires spécifiques pour les sites classés SEVESO2, les zones ATEX3, etc. Toutes ces contraintes doivent être clairement identifiées dès l'expression du besoin.

Annexe F
Contraintes règlementaires concernant la vidéoprotection

Les formalités règlementaires à accomplir peuvent varier en fonction des lieux qui sont filmés.

F.1 Lieu non ouvert au public

Si les caméras filment un lieu non ouvert au public (lieux de stockage, réserves, zones dédiées au personnel), aucune formalité auprès de la CNIL n'est nécessaire. Si l'organisme qui a mis en place des caméras a désigné un Délégué à la protection des données (DPO), ce dernier doit être associé à la mise en œuvre des caméras. Si le dispositif doit faire l'objet d'une analyse d'impact (AIPD), le DPO doit y être associé. L'employeur doit inscrire ce dispositif de vidéoprotection dans le registre des traitements de données qu'il doit tenir.

F.2 Lieu ouvert au public

Si les caméras filment un lieu ouvert au public (espaces d'entrée et de sortie du public, zones marchandes, comptoirs, caisses), le dispositif doit être autorisé par le préfet du département (le préfet de police à Paris). Le formulaire peut être retiré auprès des services de la préfecture du département ou téléchargé sur le site du ministère de l'Intérieur. Il peut également être rempli en ligne sur le site mis à disposition par le ministère [53].

F.3 Auprès des instances représentatives du personnel

Comme dans le cas de la mise en place d'un système de contrôle d'accès physique, la mise en place d'un système de vidéoprotection implique un changement des conditions de travail. Les instances représentatives du personnel doivent donc être informées et consultées avant toute décision concernant l'installation de caméras.

F.4 Information pour un dispositif de vidéoprotection sur les lieux de travail

Les personnes concernées par la présence de dispositifs de vidéoprotection (personnels, agents, visiteurs occasionnels, etc.) doivent être informées en utilisant deux niveaux d'information :

53. https ://www.televideoprotection.interieur.gouv.fr.

- premier niveau de l'information sur des panneaux placés dans les locaux de l'entité ;
- deuxième niveau de l'information dans le règlement intérieur de l'entité, un avenant au contrat de travail, une note de service, etc..

F.5 Les textes de référence

- Le règlement général sur la protection des données à caractère personnel (règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016), lorsque les caméras sont installées dans des lieux non ouverts au public ;
- Le code de la sécurité intérieure :
  - Articles L. 223-1 et suivants (lutte contre le terrorisme),
  - Articles L. 251-1 et suivants (lorsque les caméras filment des lieux ouverts au public) ;
- Le code civil :
  - article 9 (protection de la vie privée) ;
- Le code pénal :
  - Article 226-1 (enregistrement de l'image d'une personne à son insu dans un lieu privé),
  - Article 226-18 (collecte déloyale ou illicite de données à caractère personnel),
  - Article 226-20 (durée de conservation excessive des données à caractère personnel),
  - Article 226-21 (détournement de la finalité du dispositif),
  - Article R. 625-10 (absence d'information des personnes concernant leurs données à caractère personnel collectées) ;
- Le code du travail :
  - Article L. 2312-38 (moyens de contrôle de l'activité des salariés),
  - Articles L. 1221-9 et L. 1222-4 (information individuelle des salariés),
  - Article L. 1121-1 (principe de proportionnalité).

Information

Les informations de cette annexe sont directement issues du document de la CNIL intitulé « la vidéosurveillance-vidéoprotection au travail »[54].

54. https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf.

Liste des recommandations

Bibliographie

[1] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[2] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[3] *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*.
Guide ANSSI-BP-043 v1.0, ANSSI, août 2018.
https://www.ssi.gouv.fr/guide-802-1X/.

[4] *Externalisation et sécurité des systèmes d'information - Un guide pour maîtriser les risques*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

[5] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

[6] *La défense en profondeur appliquée aux systèmes d'information*.
Guide Version 1.1, ANSSI, juillet 2004.
https://www.ssi.gouv.fr/defense-profondeur.

[7] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[8] *Recommandations de sécurité pour la mise en œuvre de dispositifs de vidéoprotection*.
Note technique 524/ANSSI/SDE, ANSSI, février 2013.
https://www.ssi.gouv.fr/nt-videoprotection/.

[9] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[10] *Recommandations de sécurité relatives à TLS*.
Guide SDE-NT-035 v1.1, ANSSI, août 2016.
https://www.ssi.gouv.fr/nt-tls.

[11] *Cartographie du système d'information - Guide d'élaboration en 5 étapes*.
Guide, ANSSI, 2018.
https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/.

[12] *EBIOS Risk Manager*.
Guide, ANSSI, 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/.

[13] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[14] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios/.

[15] *Instruction générale interministérielle n° 1300*.
Référentiel Version 1.0, ANSSI, novembre 2011.
https://www.ssi.gouv.fr/igi1300/.

[16] *RGS : Annexe B2 Gestion des clés cryptographiques*.
Référentiel Version 1.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[17] *RGS : Référentiel Général de Sécurité*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[18] *Instruction interministérielle n°300 - Protection contre les signaux compromettants*.
Référentiel, SGDSN/ANSSI, 2014.
https://www.ssi.gouv.fr/entreprise/reglementation/reglementation-technique/instruction-interministerielle-n-300sgdsnanssi-sur-la-protection-contre-les-signaux-compromettants.

[19] *RGS : Annexe B1 Mécanismes cryptographiques*.
Référentiel Version 1.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[20] *Instruction interministérielle n° 901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901/.

[21] *Prestataires d'audit de la sécurité des systèmes d'information – référentiel d'exigences*.
Référentiel Version 2.1, ANSSI, octobre 2015.
https://www.ssi.gouv.fr/referentiel-passi.

[22] *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage – Référentiel d'exigences*.
Référentiel 3.1, ANSSI, juin 2018.
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf.

[23] *Qualification*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/qualification/.

[24] *L'accès aux locaux et le contrôle des horaires sur le lieu de travail*.
Mémo, CNIL, 2018.
https://www.cnil.fr/fr/sites/default/files/atoms/files/_travail-vie_privee_acces_locaux_controle_horaires.pdf.

[25] *Réglement type : Biométrie sur le lieu de travail*.
Mémo, CNIL, 2019.
https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf.

[26] *RGPD - Chapitre4, Article 30 - Registre des activités de traitement*.
Référentiel, CNIL, 2018.
https://www.cnil.fr/reglement-europeen-protection-donnees/chapitre4#Article30.

[27] *RGPD - Chapitre4, Article 35 - Analyse d'impact relative à la protection des données*.
Référentiel, CNIL, 2018.
https://www.cnil.fr/reglement-europeen-protection-donnees/chapitre4#Article35.

[28] *Contrôle d'accès - Document technique pour la conception et l'installation*.
Guide, CNPP.
https://www.cnpp.com/.

[29] *Cybersécurité - Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique*.
Guide, CNPP.
https://www.cnpp.com/.

[30] *Vidéosurveillance - Règles d'installation*.
Guide, CNPP.
https://www.cnpp.com/.

[31] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[32] *Cisco Systems' Private VLANs : Scalable Security in a Multi-Client Environment*.
Memo, IETF, 2010.
https://tools.ietf.org/html/rfc5517/.

ANSSI-PA-72
Version 2.0 - 04/03/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN