**Une image contenant texte

Description générée automatiquement**

**Recommandations sécurité dans le cadre du renouvellement des systèmes de contrôle d’accès et de vidéoprotection des sites/datacenters**

|  |
| --- |
|  |
|  |

*Sommaire*

[1 Contexte 4](#_Toc173144559)

[2 Objectifs - Niveau de sécurité cible 5](#_Toc173144560)

[3 Hypothèses 6](#_Toc173144561)

[4 Recommandations générales - Partitionnements/Isolations réseau 9](#_Toc173144562)

[5 Recommandations particulières réseaux et communications 10](#_Toc173144563)

[5.1 Recommandations sur les infrastructures réseaux et communications : 10](#_Toc173144564)

[6 Recommandations particulières des Badges - UTL - Station - GAC 11](#_Toc173144565)

[6.1 Technologie sans contact autorisée 11](#_Toc173144566)

[6.2 Authentification mutuelle cryptographique et protection des échanges 11](#_Toc173144567)

[6.3 Informations fonctionnelles du badge 11](#_Toc173144568)

[6.4 Clés cryptographiques diversifiées et Algorithmes éligibles 12](#_Toc173144569)

[6.5 Partitionnement des clés cryptographiques d'authentification 12](#_Toc173144570)

[6.6 Protection des clé maitresses 13](#_Toc173144571)

[6.7 Sécurisations des stations / GAC 13](#_Toc173144572)

[7 Recommandations particulières du Système de vidéo surveillance 14](#_Toc173144573)

# Contexte

La SDSSI a cadré les exigences et préconisations techniques en regard des infrastructures de gestion de contrôle d’accès et vidéoprotection pour les bâtiments hébergeant des datacenters.

Cette démarche rentre dans le cadre d’un renouvellement de marché de ce type d’outil au Datacenter de Lyon (69).

Ce document a donc pour but de formaliser les exigences et préconisations techniques en regard des infrastructures de gestion de contrôle d’accès et vidéoprotection d’un bâtiment Datacenter de la DSI ACOSS.

Il doit également permettre à la chaine de destinataires de pouvoir exprimer une partie des critères concernant ces périmètres au sein des documents du futur appel d’offre.

Légende couleur du texte surligné :

A compléter par les destinataires

A modifier/compléter par PRSD

Eléments structurants/importants

# Objectifs - Niveau de sécurité cible

**Objectifs :**

L’analyse de PRSD se base en grande partie sur le document ANSSI « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et vidéoprotection - v2.1.pdf ». Ce guide définit les recommandations à suivre pour acquérir et mettre en œuvre de façon sécurisée un système de contrôle d’accès et de vidéoprotection des Bâtiments de nos Datacenter (Lyon et Toulouse).

Le présent document ne « reprend pas » l’ensemble des recommandations du guide de l’ANSSI mais décrit des recommandations « adaptées » au(x) contexte(s) de l’Acoss et jugées essentielles à la construction sécurisée d’un système de contrôle d’accès et de vidéo surveillance. Il conviendra cependant de suivre l’ensemble des recommandations du guide de l’ANSSI pour construire un système de contrôle d’accès et de vidéo surveillance d’un niveau de sécurité adapté à la protection de nos datacenters.

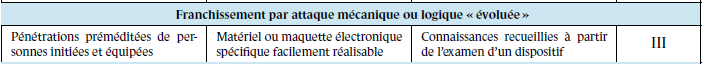
Le présent document ne traitera pas en détail des différentes zones ou cartographie à traiter, ni des valeurs métiers et inventaire des biens à protéger, ce rôle relève des services gestion bâtiment [R2, R3, R4 et R5] destinataires du présent document.

**Niveau de sécurité cible** :

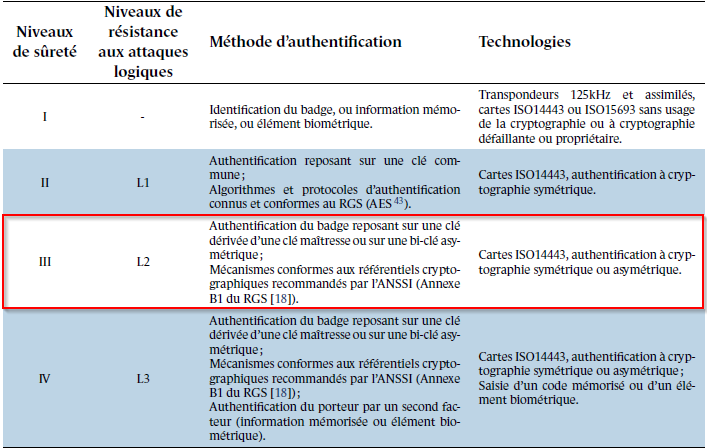
Premièrement il faut déterminer un niveau de sureté [R6] en rapport avec les types de menaces potentielles pour pouvoir préconiser ou exiger ce qui est adéquat.

Le choix sur le niveau de sureté est le niveau 3 (Le niveau 4 est le plus haut et 1 le plus bas).





Ce niveau de sureté de 3 implique alors un niveau de résistance aux attaques logiques de niveau L2



# Hypothèses

**Zones protégées par niveau de sensibilité** :

Ceci est une proposition qu'il conviendra d'adapter. Ces zones permettront de proposer un partitionnement des badges sans contact (DESFire) correspondant à ces niveaux de sensibilités afin de mieux protéger les clé secrètes d’accès aux zone sensibles.

Classement de la zone la plus critique à la moins sensible (à réévaluer avec le titulaire du march) :

Sites Datacenters :

* Sensibilité 3 : Critique : Salle(s) serveurs et Réseaux du Datacenter
* Sensibilité 2 : Critique technique : Salles critiques techniques du Datacenter
* Sensibilité 1 : Sensible : Zone à accès protégé de niveau sensible (bureaux, salles de réunion, ...)
* Sensibilité 0 : Semi-publique : Accès Parking et zone publique du bâtiment

Ces zones seront déclinées par site.

**Porteurs des badges** : Badges d’accès destinées (principalement) à des salariés Acoss et à du personnel "externe"

**Vocabulaire du document** :

**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 (GAC)**

Le centre de gestion des contrôles d’accès, également appelé GAC, 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.

**Station d’enrôlement**

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

**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.

**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 (VMS)**

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.

**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.

**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.

# Recommandations générales - Partitionnements/Isolations réseau

* Chaque datacenter Lyon et Toulouse dispose de son propre système de contrôle d'accès physique. Les 2 systèmes sont totalement indépendants et non connectés entre eux.
* Le réseau du système de contrôle d'accès doit à minima être isolé logiquement du réseau de l'Acoss (cf Spécifications détaillées « D.4 Réseaux et communication » doc. ANSSI, page 99).
* L'ensemble du système de contrôle d’accès considéré comme très sensible devra être hébergé au sein d'une (nouvelle) zone réseau protégée du réseau de l'Acoss par un pare-feu.
* Ce système ne sera pas accessible depuis le réseau de l'Acoss (aucun flux entrant autorisé) à l’exception des flux d’administration à condition que ceux-ci soient initiés du réseau d’administration par des stations d’administration dédiées et durcies.
* Tous les flux sortant de cette nouvelle zone réseau vers le réseau de l'Acoss et vers internet devront être filtrés en points à points (seuls les flux nécessaires et suffisant doivent être autorisés)
* Les stations (Windows) du système de contrôle d’accès devront être dédiées sans accès à Internet.
* L’acquisition de composants/produits qualifiés par l’ANSSI [R1] en dernières versions est recommandée.
* Pour les badges sans contact MIFARE DESFire EV2 ou EV3, la certification « Critères Communs EAL5+ » est demandée.

# 

# Recommandations particulières réseaux et communications

En regard du niveau L2 de résistance aux attaques logiques à atteindre, voici les exigences L1+L2 à respecter afin d’atteindre ce niveau.

## Recommandations sur les infrastructures réseaux et communications :

* Les cheminements de câbles sont mis en place à l’intérieur des zones contrôlées.
* Les liaisons de communication entre les moyens physiques d’ouverture et l’UTL sont des liaisons dédiées au système de sécurité.
* Les liaisons filaires sont surveillées de manière à garantir qu’aucune tentative de fraude ne puisse être réalisée.
* La perte d’informations au niveau des liaisons doit être signalée et traitée comme une alarme.
* La fibre optique doit être privilégiée pour les liaisons entre bâtiments.
* La transmission des informations du système de contrôle d’accès se fait sur un réseau logique dédié à ce système.
* Les protocoles de communication utilisés (algorithmes de chiffrement inclus) doivent être décrits, et particulièrement les principes de sécurisation et de vérification des échanges.
* 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.
* La communication entre l’UTL et le GAC doit être chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l’ANSSI.

N.B1 : Dans le cas des datacenter de l’URSSAF CAISSE NATIONALE un investissement d’un cluster de pare-feux dédié (1 cluster par Datacenter) sera à prévoir afin de décoréler le filtrage des flux des solutions de contrôle d’accès et de vidéoprotection du reste des Firewall Datacenter (indépendance lors des maintenances et coupures par rapport aux Firewall Datacenter).

N.B2 : La mise en place de 4 vlan dédiés sera necessaire : 1 vlan GAC, 1 (ou N selon niveau de sécurité) vlan UTL, 1 vlan VMS (Appliance/Hyperviseur dédié ou SIE) , 1 (ou N selon niveau de sécurité) vlan cameras-radars.

* Dédier une station de gestion GAC et une autre VMS, dans le même vlan respectifs que les serveurs GAC et VMS, afin de ne pas utiliser le poste bureautique Acoss. Possibilité d’utiliser un rebond dédié passant via l’outils RAMSES à partir du réseau d’administration.
* Utiliser des comptes locaux
* Ne pas mettre en place une solution de télémaintenance vers les serveurs GAC ou VMS [R89]
* Administrer techniquement les équipements des centres de gestion de systèmes de contrôle d’accès ou de vidéoprotection depuis un réseau d’administration dédié à cet effet sinon utiliser le réseau d’amin du SI [R80] : étudier le moment venu si il sera possible de s’appuyer sur le SIE/SIA.
* Distinguer les comptes d’administration métier (configuration) des comptes métiers (utilisateurs).
* Assurer la MCO et MCS des composants d’infrastrutures concernés ainsi que la journalisations des logs associés.

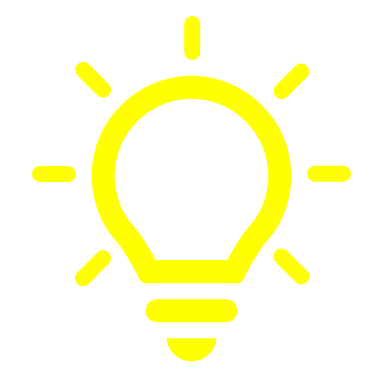
# Recommandations particulières des Badges - UTL - Station - GAC

## Technologie sans contact autorisée

- Seule la puce sans contact MIFARE DESFire (EV2 ou EV3) est autorisée pour permettre un contrôle d'accès sécurisé au datacenter. La puce sans contact MIFARE CLASSIC est proscrite pour cet usage

## Authentification mutuelle cryptographique et protection des échanges

* L'authentification mutuelle cryptographique du badge et de l'UTL est requise
* Toute identification "simple" (UID) du badge vis à vis de l'UTL est proscrite
* Tous les échanges entre le badge et l'UTL devront être protégés en confidentialité (chiffrement) et en intégrité
* Le lecteur est transparent dans les échanges et agit comme simple relais de données "opaques" (échanges chiffrées). Il n'héberge aucune clé cryptographique

*Correspond à la "Configuration type n°1 : tête de lecture transparente, authentification de bout en bout" du guide de l'ANSSI (R41, chapitre 6.5.1, page 51)*

## Informations fonctionnelles du badge

* Il faudra veiller à minimiser les informations présentes sur les badges (ANSSI R32) :
  + Informations imprimées sur le badge
  + Informations inscrites dans la puce sans contact MIFARE DESFire

Informations imprimées sur le badge :

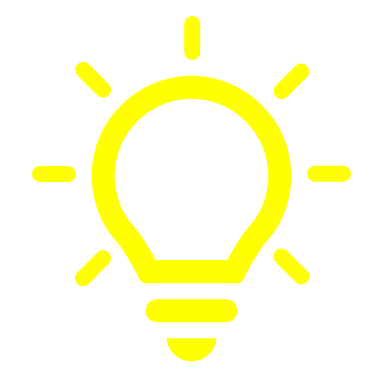
* Un numéro de traçabilité à des fins administratives différent du numéro d’identification inscrit dans la puce
* Aucune information sur le porteur à l'exception de sa photo
* Aucune information sur les autorisations du porteur.
* Aucune information sur l'entreprise

Informations inscrites dans la puce sans contact MIFARE DESFire :

* La puce sans contact ne devra contenir que les éléments strictement nécessaires aux phases d’identification et d’authentification, à savoir :
* Un identifiant unique UID du badge (numéro de série du badge - non modifiable)
* Un numéro d’identification unique associé au porteur du badge
* Aucune autre information ne doit être inscrite au sein de la puce sans contact.
* Le numéro d’identification unique associé au porteur sera généré par l'application de contrôle d'accès lors de l'enrôlement du badge. Ce numéro d’identification sera enregistré sur la puce sans contact et protégé par la clé d'authentification diversifiée de l'application.

## Clés cryptographiques diversifiées et Algorithmes éligibles

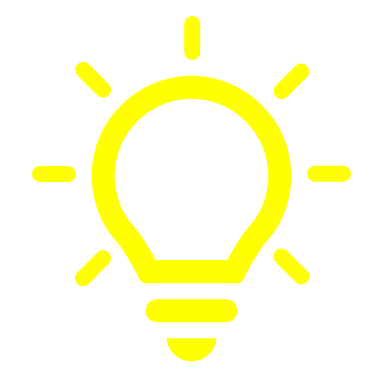
* Les clés cryptographiques de chaque datacenter doivent être distinctes (aucune clé "commune" aux 2 systèmes de contrôle d'accès)
* Une nouvelle clé maitre (master key) de configuration propre à chaque datacenter (Lyon et Toulouse) sera générée (par défaut les badges possèdent un secret unique "Acoss" initialisé par le fournisseur de badges)
* Seules des clés cryptographiques diversifiées seront injectées/paramétrées au sein des badges

*Permet de limiter, en cas de compromission des clés d'un badge, que l'ensemble des cartes émises soient compromises*

* Les clés et algorithmes employés devront être conformes au "Référentiel Général de Sécurité Annexe B1" :
  + Les clés de chiffrement symétrique DES ou ses variantes (3DES,...) sont proscrites
  + L'algorithme AES 128 bits sera privilégié

## Partitionnement des clés cryptographiques d'authentification

* Il est fortement recommandé qu'à chaque niveau de sensibilité soit associée une clé d'authentification maitresse distincte (ANSSI R58 page 65)

 *Un badge ne dispose que des seules clés d'authentifications (diversifiées) nécessaires à son usage. Par ex. un badge ne permettant l'accès qu'à une zone non sensible, ne pourra pas s'authentifier auprès d'un UTL d'une zone sensible et ce quelles que soient les autorisations de son porteur. D'autre part en cas de vol ou perte, le badge ne contiendra aucune clé d'accès aux zones sensibles.*

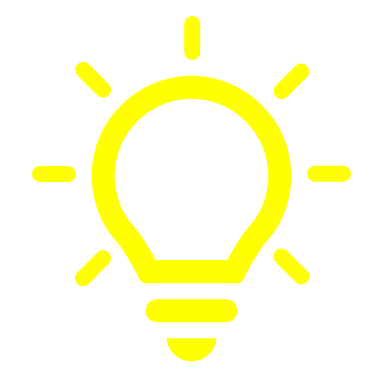
*En "contrepartie", si le porteur doit être autorisé à accéder à une zone sensible après l'enrôlement initial du badge, celui-ci devra être maj (station d'enrôlement) pour injecter la nouvelle clé d'authentification de la zone sensible (versus maj des autorisations sans nécessité le retour du badge).*

*Chaque niveau de sensibilité correspond(ra) à une "application" distincte du badge sans contact MIFARE DESFire*

*Dans le cas - inverse - d'un secret maitre d'authentification unique et commun aux zones de différentes sensibilité, chaque UTL pourra authentifier n'importe quel badge et devra ensuite vérifier les autorisations d'accès de son porteur.*

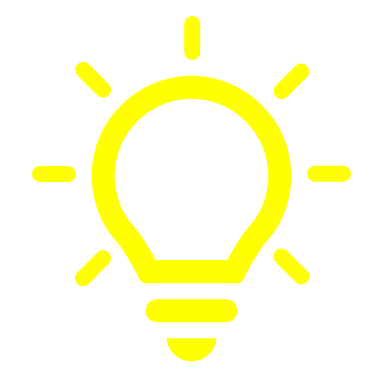
## Protection des clé maitresses

* Il est essentiel de protéger/sécuriser strictement le stockage et l'accès aux différentes clés maitresses. Sans cela, la sécurité du contrôle d'accès aux datacenters pourrait être compromise.
* Toute personne autorisée à accéder logiquement à une clé maitresse devra être authentifiée fortement, par ex. à l'aide de sa carte Sesame
* Une traçabilité stricte des accès aux clés maitresses devra être mise en place
* Les clés maitresses devront être séquestrées au sein d'un boitier HSM
* Lorsque cela est possible ces clés devront être mises "hors ligne" (déconnectées du réseau) et protégées

*Par ex. la divulgation d'une clé maitresse d'authentification pourrait permettre de cloner une nouvelle carte pirate à partir de n'importe quelle carte existante. Cette carte pirate permettrait de s'authentifier auprès de n'importe quel UTL associé au niveau de sensibilité de la clé compromise*

**UTL :**

* L'UTL devra être localisé à l’intérieur de la zone contrôlée au sein d'une zone sécurisée fermée (ANSSI R38)
* L'usage d'un module matériel SAM (Secure Access Module) associé à chaque UTL est requis (ANSSI R57)

*Le module matériel SAM permet de séquestrer une clé maitresse d'authentification (à l'image d'un boitier HSM) et de générer pour le compte de l'UTL une clé diversifiée nécessaire à l'authentification d'un badge*

## Sécurisations des stations / GAC

**Station d’enrôlement des badges :**

* Elle devra être traitée d'un point de vue de la sécurité comme une station d'administration
* Elle devra être dédiée à cet usage à l'identique d'un poste d'administration
* Elle devra être connecté au réseau logique dédié du système de contrôle d'accès (prise réseau dédiée)
* Elle devra être durcie, maintenue en condition de sécurité et non connecté à internet
* Elle devra être localisée au sein d'une zone sécurisée fermée de sensibilité élevée
* Tous les flux de la station vers un service de gestion du système de contrôle d'accès (GAC) devront être chiffrés avec une authentification forte du client et du service accédé (serveur). Par ex. authentification forte mutuelle HTTPS de l’utilisateur et du serveur distant accédé à l’aide de la carte Sesame et du certificat serveur.
* Une traçabilité fine des accès à la station d’enrôlement et opérations devra être mise en place.
* L'administration technique de la station devra être effectuée à partir d'un poste d'administration durci et dédié du réseau d’administration de l’Acoss.
* La télémaintenance de la station depuis internet est prohibée.

**Centre de gestion du système de contrôle d'accès (GAC) :**

* Le système d'exploitation des serveurs du centre de gestion devra être durci et maintenu en condition de sécurité.
* Tous les flux vers un serveur ou depuis un serveur vers un service distant devront être chiffrés et authentifiés (par ex. auth. HTTPS du serveur ou du service distant à l'aide d'un certificat du serveur ou du service distant)
* L'administration métier du Centre de gestion du système devra authentifier fortement ses administrateurs (par ex. à l'aide de la carte Sesame)
* L'administration métier du GAC devra être effectuée à partir d'un poste d'administration dédié, durci, connecté au réseau logique du système de contrôle d'accès (prise réseau dédiée) et localisé au sein d'une zone sécurisée fermée de sensibilité élevée.
* Tous les flux d’administrations métier devront être chiffrés avec une authentification forte du client et du service accédé (serveur). Par ex. authentification forte mutuelle HTTPS de l’utilisateur et du serveur distant accédé à l’aide de la carte Sesame et du certificat serveur.
* L'administration technique du GAC devra être effectuée à partir d'un poste d'administration durci et dédié du réseau d’administration de l’Acoss.
* Une traçabilité fine des accès et opérations devra être mise en place.
* La télémaintenance du GAC depuis internet est prohibée.

# Recommandations particulières du Système de vidéo surveillance

Les recommandations pour le VMS et ses stations de gestions sont similaires à celles du GAC et de ses stations de gestions citées ci-dessus.