

**Maintenance préventive et corrective des
installations de sûreté dans les établissements du
ressort de la Direction Interrégionale des Services
Pénitentiaires Grand-Ouest**

**C.C.T.P. - ANNEXE 07 – PSSI Sûreté spécifique
(Politiques de sécurité des systèmes d'information)**

**Ministère
de la Justice**



Direction de
l'administration
pénitentiaire

PSSI SURETE

VOLET SI SPECIFIQUES

(PSSI-DAP-SUR)

Version 0.8 – mars 2023

Fiche de contrôle du document

Caractéristiques du document

Identification :	RI03-PSSI_Surete_Specifique-0.8.docx
Objet :	PSSI Sureté - Spécifique
Version :	Version 0.8 du 14/03/2023

Contributeurs

NOM Prénom (trigramme)	Fonction
David DU SERRE-TELMON (DST)	Consultant SSI du pôle SSI DAP
Bernard CASSOU-MOUNAT (BCM)	RCSSI DAP
Franck PERREAU (FPE)	RCSSI Adjoint DAP

Suivi des versions

Version	Date	Rédacteur	Relecteur	Modification
0.1	27/04/2022	DST		Rédaction de la version initiale du document
0.2	02/05/2022	DST	DDST	Modifications à la suite de relecture interne
0.3	05/05/2022	DST		Modifications suite à entretien avec les métiers.
0.4	09/05/2022	DDST		Correction forme
0.5	29/06/2022	DDST	FPE	Relecture et correction avant publication
0.6	05/09/2022	DDST	FPE BCM	Intégration des exigences ANSSI Vidéosurveillance
0.7	07/03/2023	DDST		Mise à jour des exigences biométrie et GTC/GTB
0.8	14/03/2023	DDST	BCM	Mise à jour mineure sur les numéros d'annexe

Processus de validation

Émetteur/Rédacteur	Approbateur
Nom : Pôle SSI DAP Date : 14/03/2023	Nom : Bernard CASSOU-MOUNAT Date : 14/03/2023
Validation finale : Laurent RIDEL (DAP) Date :	

Sommaire

Partie 1	Cadre d'emploi	5
	Avant-propos	6
1.1	Objet et champ d'application de la PSSI Sureté spécifique	6
Partie 2	Règles de sécurité.....	7
2.1	Gestion technique centralisée (GTC/GTB)	8
2.1.1	Introduction	8
2.1.2	Gestion de l'exploitation et de la maintenance	9
2.2	Système de vidéosurveillance	10
2.2.1	Introduction	10
2.2.2	Gestion des biens.....	11
2.2.3	Sécurité physique et environnementale	12
2.2.4	Gestion de l'exploitation et de la maintenance	12
2.2.5	Contrôle d'accès	13
2.3	Systèmes de gestion des accès.....	14
2.3.1	Introduction	14
2.3.2	Gestion des biens.....	15
2.3.3	Sécurité physique et environnementale	18
2.3.4	Gestion de l'exploitation et de la maintenance	19
2.4	Ouvertures électro commandées.....	21
2.4.1	Introduction	21
2.4.2	Gestion des biens.....	21
2.4.3	Gestion de l'exploitation et de la maintenance	22
2.5	Système de contrôle d'accès aux parloirs	23
2.5.1	Introduction	23
2.5.2	Gestion des biens.....	23
2.5.3	Sécurité physique et environnementale	24
2.5.4	Contrôle d'accès	24
2.5.5	Gestion de l'exploitation et de la maintenance	25
2.6	Détection périmétrique.....	26
2.6.1	Introduction	26
2.6.2	Sécurité physique ou environnementale	26
2.7	Gestion des clés.....	27
2.7.1	Introduction	27
2.7.2	Contrôle d'accès	27

2.7.3	Gestion de l'exploitation et de la maintenance	27
-------	--	----

Partie 1 Cadre d'emploi

Avant-propos

Le présent document fait partie de l'ensemble documentaire découlant de la PSSI des systèmes d'information de sûreté pénitentiaire. Il est complémentaire à la *PSSI Sûreté* [RI.01] (PSSI-DAP-SUR) et n'est pas autoporteur.

La DAP dispose d'un *Glossaire des sigles et dictionnaire des termes référencés* [RI.05] ainsi que d'un *Corpus documentaire de référence*, unifié et normalisé, référencé [RI.04].

Les références entre crochet [REF] figurant dans le présent document renvoient à ce corpus documentaire.

Sauf mention contraire, ce document ainsi que les documents de référence qui y sont recensés sont librement consultables et peuvent être obtenus sur simple demande auprès du RCSSI de la DAP.




1.1 Objet et champ d'application de la PSSI Sûreté spécifique

Le périmètre est identique à celui de la PSSI-DAP-SUR, qu'elle complète.

La présente PSSI compile les règles spécifiques à un sous-ensemble des systèmes d'information de sûreté pénitentiaire qui ne sont par définition pas transverses et donc absentes de la PSSI-DAP-SUR.

La plupart des exigences décrites dans cette PSSI sont directement applicables dans chaque projet et système d'information de sûreté. Elles constituent ainsi le cahier des charges SSI général destiné à assurer un socle minimal en matière de sécurité numérique. En fonction des besoins de sécurité du SI qui sera à homologuer, il pourra être nécessaire de rédiger une PSSI spécifique si les besoins de sécurité sont plus contraignants sur ce périmètre.

Ces exigences sont formalisées de la manière suivante :

XXX000 : Titre de l'exigence	
  	Exigence globale applicable à tout système d'information de sûreté de la DAP.

DAP



Prestataire



DAP et Prestataire



Les exigences applicables au prestataire portent sur son SI ainsi que sur celui de la DAP pour lequel il est missionné.

Partie 2 Règles de sécurité

2.1 Gestion technique centralisée (GTC/GTB)

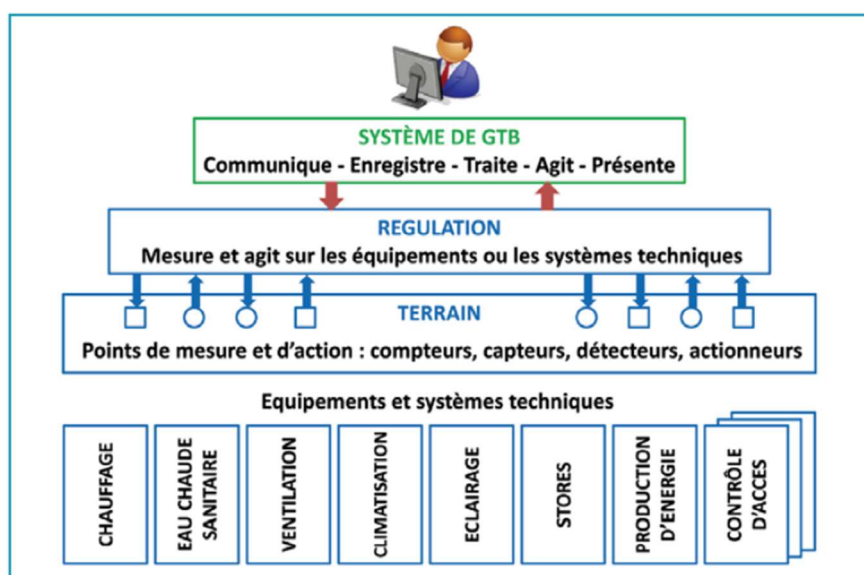
2.1.1 Introduction

La supervision par la gestion technique centralisée (GTC) permet de piloter à distance l'ensemble des éléments d'installations d'un seul domaine technique comme :

- la distribution d'électricité ;
- les dispositifs incendie (alarmes, extinction) ;
- les équipements de chauffage ;
- les équipements de froid (réfrigérateurs, climatisation) ;
- les monte-charges et ascenseurs ;

La gestion technique du bâtiment (GTB) est le niveau supérieur de la GTC. Ce système est capable de gérer plusieurs périmètres techniques d'un même bâtiment et supervise l'ensemble des informations sur un outil de gestion commun. Quels que soient les différents équipements (chauffage, climatisation, électricité, sécurité), les domaines techniques sont pilotés de manière homogène et centralisée.

Sur le schéma ci-dessous¹, le volet GTB est représenté en vert, tandis que le volet GTC correspond aux modules en bleu.



Le système de GTB permet de centraliser la gestion des équipements techniques
(source : Guide RAGE - juin 2014)¹

Que l'on travaille à l'échelle d'un logement ou d'un bâtiment entier, la gestion centralisée fonctionne toujours selon le même principe. Voici les 4 éléments essentiels à la réalisation d'une GTB/GTC² :




- Capteurs : permettent d'acquérir une information qui sera ensuite traitée par informatique. Par exemple : capteur de lumière ou capteur de présence,
- Actionneurs : va traduire au niveau local un ordre provenant de l'interface de gestion,

¹ <https://www.banquedesterritoires.fr/sites/default/files/2018-11/Cerema%20fiche%206.pdf>

² <https://www.mapes-pdl.fr/wp-content/uploads/2020/04/IDELEC-GTC-GTB.pdf>

- Scénarios programmés : ensemble de conditions qui, lorsqu'elles sont réunies, mettent en action une commande. Exemple : Réduire de moitié la lumière lorsqu'il n'y a personne dans la pièce ou, le cas échéant, entre 20h et 8h du matin,
- Interface de gestion : logiciel qui permet de récupérer des informations liées à la consommation et à la bonne marche des appareils. L'interface rend aussi possible l'implémentation des scénarios.

2.1.2 Gestion de l'exploitation et de la maintenance

GTCEXP01 : Cloisonnement du SI GTC/GTB vis-à-vis des SI de sûreté	
	<p>Les services du SI GTC/GTB sont complètement indépendants des SI de sûreté et doivent être isolés physiquement.</p> <p>Néanmoins, dans certains cas, certaines mutualisations physiques restent possibles pour rationaliser les coûts d'infrastructure et de maintenance, comme le partage des équipements de cloisonnement, du réseau d'interconnexion, de l'équipe d'exploitation. Dans tous les cas, le cloisonnement logique doit être observé et aucune communication réseau IP ne doit-être possible entre les réseaux sur le site.</p> <p>Ces mutualisations sont soumises à validation du RCSSI de la DAP.</p>
GTCEXP02 : Remontée d'information de la GTC/GTB vers la sûreté	
	<p>Le SI GTC/GTB peut mettre à disposition de la gestion centralisée des alarmes (GSA) du SI de sûreté des états par l'intermédiaire de contacts secs (les communications IP sont proscrites).</p>
GTCEXP03 : Supervision du SI GTC/GTB sur site	
	<p>Le système doit être supervisé en permanence par du personnel sur site, afin de traiter dans les plus brefs délais les alarmes impactant la sécurité des biens et des personnes.</p>

2.2 Système de vidéosurveillance

2.2.1 Introduction

La vidéosurveillance a pour vocation d'être un outil de levée de doute et de renforcement du contrôle des circulations, des cours, des terrains de sport et des zones à risques en et hors détention.

Généralement ce système est utilisé en association avec :

- la gestion des accès afin d'identifier le demandeur de l'accès vers le poste d'hébergement (PH) et plus généralement le poste protégé de la zone pendant la journée, avec un report au poste central de sécurité (PCS) la nuit ;
- la supervision pour vérification, identification de l'alarme et enregistrement de l'incident ;
- l'interphonie, pour l'enregistrement des communications.

Ainsi, l'ensemble de la chaîne (caméra, réseau, serveur et poste client) répond à cet objectif.

2.2.2 Gestion des biens

VIDGDA01 : Description des processus organisationnels de vidéosurveillance



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.

L'absence de processus organisationnels est généralement source d'approximations dans la pertinence des droits d'accès affectés aux usagers et dans l'attribution des droits d'utilisation aux opérateurs VMS.

VIDGDA02 : Cartographie du système de vidéosurveillance



Comme tout SI de sûreté, le SI de vidéosurveillance doit faire l'objet d'une cartographie par l'intégrateur. Cette cartographie doit contenir au minimum les éléments suivants :

- schéma représentant les zones à protéger/contrôler et le niveau attendu de leur protection ;
- 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 (caméras, VMS, 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 administrateurs.

VIDGDA03 : Mécanismes de chiffrement des vidéos sur le disque



Il est fortement recommandé de privilégier des solutions de vidéosurveillance proposant des protocoles standards de chiffrement pour la sécurisation des vidéos sauvegardées sur disque. Il convient de privilégier des protocoles qualifiés quand les solutions les implémentent.

La solution choisie doit également offrir la possibilité de s'intégrer dans une infrastructure de gestion de clés propre à l'entité.

Les algorithmes d'intégrité et de chiffrement mis en œuvre doivent respecter les préconisations mentionnées dans le *référentiel général de sécurité [RRG.01]* publié par l'ANSSI.

2.2.3 Sécurité physique et environnementale

VIDPHY01 : Support physique dédié 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.

VIDPHY02 : Cloisonnement logique pour les 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 (802.1X)

2.2.4 Gestion de l'exploitation et de la maintenance

VIDEXP01 : Protection des interfaces locales d'administration des caméras



Les interfaces locales d'administration doivent être sécurisées. Les moyens suivants doivent être mis en place :

- désactivation de l'interface locale dans la mesure du possible ;
- remplacement des mots de passe par défaut ;
- désactivation des fonctionnalités d'administration non utilisées.

VIDEXP02 : Mise à disposition des enregistrements aux autorités compétentes



Il doit être possible de mettre à disposition des autorités compétentes des images exploitables (certifiées comme non modifiées, de qualité suffisante et horodatées correctement), conformément au cadre légal et réglementaire.

VIDEXP03 : Extraction d'enregistrements vidéo



La récupération administrative ou sur réquisition d'extractions vidéo doit se faire par un intervenant nommément autorisé par le chef d'établissement, avec un compte nominatif, en se basant une procédure formalisée, afin de garantir :

- la traçabilité des actions ;
- la prévention d'éventuelles propagations virales ;
- les accès non autorisés aux enregistrements.

2.2.5 Contrôle d'accès

VIDGAC01 : Protection des enregistrements



La confidentialité et l'intégrité des enregistrements doivent être garanties au plus tôt par un mécanisme de chiffrement pour empêcher un accès non autorisé aux données (y compris l'exploitant), dans la limite des capacités techniques de la solution.

2.3 Systèmes de gestion des accès

2.3.1 Introduction

Les systèmes de gestion d'accès permettent une centralisation de l'attribution, la révocation, le suivi et la journalisation des accès physiques.

Les systèmes de gestion d'accès sont généralement composés des éléments suivants :

- Les éléments d'enrôlement et gestion des autorisations :
 - poste(s) de création de badges et d'attribution des autorisations ;
 - imprimante(s) à badges ;
 - lecteur(s)/encodeur de badges ;
 - serveur(s) de gestion d'accès.
- Les éléments de surveillance et de suivi :
 - poste de consultation.
- Les équipements de terrain :
 - badges :
 - badges personnels : nominatifs, comportant la photos et informations liées au propriétaire;
 - badges visiteurs : banalisés, comportant identifiant numérique;
 - badges véhicules pour le personnel et les prestataires réguliers du site.
 - lecteurs de badges (tête de lecture) ;
 - serrures commandable, tripode, tourniquets.

La création des badges se fait sur un poste de personnalisation généralement implanté dans la zone administrative, au niveau du secrétariat. Les badges du système de gestion des accès sont exclusivement utilisés par le personnel de l'établissement et ses visiteurs, ils ne sont pas utilisés pour les accès des détenus.

Le système est exploité en temps réel depuis la porte d'entrée principale (PEP) et la porte d'entrée logistique (PEL) par un poste client sur lequel la création des badges n'est pas possible.

Associé aux lecteurs d'entrée / sortie de la PEP, cet écran indique la liste des personnes présentes à l'intérieur de l'établissement et a en mémoire la liste des présents en fonction du jour et de l'heure.

Le système de contrôle de gestion des accès communique uniquement avec le système gestion centralisée des alarmes (GSA), ainsi que les composants d'infrastructure.

2.3.2 Gestion des biens

ACCGDA01 : Description des processus organisationnels de contrôle d'accès



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.

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

VIDGDA02 : Cartographie du système de contrôle d'accès



Comme tout SI de sûreté, le SI de contrôle d'accès doit faire l'objet d'une cartographie par l'intégrateur. 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, 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 administrateurs.

ACCGDA03 : Limitation des informations stockées sur le badge



Les données relatives aux droits d'accès et les périodes de validité ne doivent pas être stockées sur le badge.

ACCGDA04 : Traçabilité d'attribution des badges génériques



Une traçabilité doit être mise en œuvre pour faire le lien entre un badge générique numéroté et le nom de son bénéficiaire.

ACCGDA05 : Désactivation des badges génériques après usage



Les badges génériques doivent être désactivés quand ils ne sont pas utilisés.

ACCGDA06 : Visibilité du numéro du badge



Le numéro unique de traçabilité du badge doit être visible sur le support.

ACCGDA07 : Privilégier l'utilisation de cartes d'accès certifiées AVAWAN.3



Dans la mesure du possible, 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 AVAVAN.3 doit être privilégié.

ACCGDA08 : Unicité des badges



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.

ACCGDA09 : Conformité des mécanismes cryptographiques



La mise en œuvre des mécanismes cryptographiques appliqués aux mécanismes d'identification et d'authentification des badges doit être conformes aux règles décrites dans l'annexe B1 du *Référentiel général de sécurité [RRG.01]*.

ACCGDA10 : Eviter l'utilisation de clef 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.

ACCGDA11 : Utilisation de clés différentes en fonction des types d'utilisateurs



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.).

ACCGDA12 : Utilisation du 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.

ACCGDA13 : Privilégier la différenciation 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.

ACCGDA14 : Protection des 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 [RRG.01]*, notamment celles concernant la gestion des clés cryptographiques figurant dans l'annexe B2.

ACCGDA15 : Détection des changements de clefs



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

ACCGDA16 : Anticipation du remplacement des clefs 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.

ACCGDA17 : 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 serveur (GSA).

ACCGDA17 : 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.

ACC GDA18 : Restriction des badges 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 AVAVAN.5.

ACC GDA19 : Fonctionnement autonome du contrôle de badges



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.

2.3.3 Sécurité physique et environnementale

ACC PHY 01 : Protection des lecteurs de contrôle d'accès



Les lecteurs de contrôle d'accès doivent comporter des éléments de protection tels que l'effacement des clés ou le déclenchement d'une alarme en cas d'arrachement.

ACCPHY02 : Protection des postes de gestion des badges



Les postes de création de badge et de gestion des accès doivent être situés dans une zone protégée physiquement et où les accès sont restreints et tracés.
Une authentification à double facteur doit être mise en œuvre sur ces postes.

ACCPHY03 : Connexions point à point entre les têtes de lectures et l'UTL



Il est recommandé de privilégier la mise en place de connexions point-à-point (connexion directe sans équipement intermédiaire de commutation ou de concentration) sur les liaisons entre les têtes de lecture et l'UTL.

ACCPHY04 : 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.

ACCPHY05 : Cloisonnement logique entre les UTL



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.

ACCPHY06 : Contrôle d'accès aux 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.

2.3.4 Gestion de l'exploitation et de la maintenance

ACCEXP01 : Recherche d'événements sur le système de gestion des accès



Le système de gestion d'accès doit permettre à minima de :

- réaliser des recherches multicritères sur l'historique ;
- permettre de retracer l'ensemble des accès tentés par les utilisateurs, succès et échecs.

ACC EXP02 : 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.

ACC EXP03 : Procédure d'entrée 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.

ACC EXP04 : Restriction des badges à privilèges



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.

ACC EXP05 : 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.

ACC EXP06 : Vérification des 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.

Le bon fonctionnement de cette alimentation de secours, présente dans chaque UTL, est un gage de résilience du système.

ACCEXP07 : Contrôle des dispositifs 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.

ACCEXP08 : Recherche d'événements sur le système de gestion des accès



Le système de gestion d'accès doit permettre *a minima* de :

- réaliser des recherches multicritères sur l'historique ;
- permettre de retracer l'ensemble des accès tentés par les utilisateurs, succès et échecs.

2.4 Ouvertures électro commandées

2.4.1 Introduction

La gestion des ouvertures décrite dans ce document concerne les ouvertures à distance de portes, de portails, de grilles et d'appareils élévateurs électro-commandés par un système d'écran tactile, d'une boîte à bouton répartis dans les différents postes protégés ou par l'intermédiaire de la gestion centralisée des alarmes (GSA).

Ce système nécessite une association visuelle et vocale pour permettre la prise de décision, menant à l'accord ou le refus de l'ouverture à distance par le personnel habilité.

Ci-dessous un exemple des systèmes pouvant être concernées par cette PSSI :

- serrures électriques sur les portes et grilles ;
- appareils élévateurs ;
- portails ;
- herse ;
- etc.

2.4.2 Gestion des biens

SER GDA01 : Association des systèmes de commandes et des systèmes de levée de doutes



Les systèmes de commande à distance doivent être associés aux systèmes de levée de doute vocaux et vidéos.

SERGDA02 : Utilisation du mode SAS avec les systèmes électro commandés



L'ouverture en mode SAS doit être mise en place pour les ouvertures électro commandées.

Néanmoins, une dérogation peut être émise dans le cas où ce dispositif peut nuire à la fluidité de la circulation au sein de l'établissement.

SERGDA03 : Désinhibition du mode SAS



Un bouton d'urgence doit pouvoir désinhiber le mode SAS et entraîner une alarme visuelle et sonore au niveau des différents postes protégés. La désinhibition du mode SAS doit être dûment justifié et le système doit être remis en service au plus tôt après sa désactivation.

2.4.3 Gestion de l'exploitation et de la maintenance

SEREXP01 : Suivi des actions réalisées sur le système



L'utilisateur à l'origine d'une ouverture à distance (par badge ou écran tactile depuis un poste protégé) doit être tracé.

SEREXP02 : Entretien des serrures du SAS



La procédure d'exploitation sécurisée (PES) des serrures électro commandées doit inclure la vérification et l'entretien physique régulière des serrures du mode SAS.

2.5 Système de contrôle d'accès aux parloirs

2.5.1 Introduction

Le contrôle d'accès aux parloirs a pour objectif d'éviter toute substitution de détenus lors d'entrevues dans les parloirs.



Il repose sur une solution biométrique permettant d'identifier le détenu et d'assister la mission de l'agent qui validera manuellement l'accès *in fine*.

Le système peut être couplé à un badge nominatif. Les badges détenus du contrôle d'accès aux parloirs sont complètement indépendants des badges du personnel et des visiteurs de l'établissement.

Le dispositif est généralement implémenté dans les zones suivantes :

- au Greffe : station d'enrôlement ;
- aux parloirs familles Homme (Entrée et Sortie) : lecteur biométrique ;
- aux parloirs familles (Entrée/Sortie) : lecteur biométrique ;
- aux parloirs familiaux (Entrée/Sortie) : lecteur biométrique ;
- en local technique informatique : base de données biométrique.

2.5.2 Gestion des biens

BIOGDA01 : Recommandation d'implémentation du système de contrôle d'accès	
	<p>L'implémentation du système de contrôle d'accès biométrique doit suivre les « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » de l'ANSSI [RD.19].</p> <p>Les badges détenus doivent répondre à des contraintes spécifiques en étant résilients et économiques.</p> <p>Un niveau de sécurité du badge modéré du badge est pallié par le couplage avec l'identification biométrique et la validation manuelle systématique de l'accès par un agent de la DAP.</p>
BIOGDA02 : Limitation des informations stockées sur le badge	
	<p>Les données relatives aux droits d'accès et les périodes de validité ne doivent pas être stockées sur une puce ou une bande magnétique du badge.</p> <p>Aucune information sensible ne doit être mentionnée sur le badge (ex : numéro d'écrou).</p>

BIOGDA03 : Validation du modèle biométrique



Le modèle d'identification biométrique utilisé pour le contrôle d'accès (reconnaissance palmaire, iris, faciale etc.) doit être conforme à la législation européenne (RGPD [RRG.07, directive police-justice [RRG.08]] et validé par le correspondant informatique et liberté (CIL) de la DAP.

2.5.3 Sécurité physique et environnementale

BIOPHY01 : Protection des lecteurs de contrôle d'accès



Les lecteurs de contrôle d'accès doivent comporter des éléments de protection tels que l'effacement des clés ou le déclenchement d'une alarme en cas d'arrachement.

BIOPHY02 : Protection des postes de gestion des badges



Les postes de création de badge et de gestion des accès doivent être situés dans une zone protégée physiquement et où les accès sont restreints et tracés.

Une authentification à double facteur doit être mise en œuvre sur ces postes.

BIOPHY03 : Protection physique de la base de données biométrique



La partie serveur de la solution (base de données) doit être hébergée dans un local technique inaccessible physiquement aux personnes non habilitées.

2.5.4 Contrôle d'accès

BIOGDA01 : Protection logique de la base de données biométrique



Les informations sensibles de la base de données (nom, prénom, numéro d'écrou) doivent être protégées par des mesures de sécurité logiques (filtrage des flux, compte de service spécifique, chiffrement) et décrites dans le dossier d'architecture de la solution.

BIOGDA02 : Enrôlement de l'information biométrique



Lors de l'enrôlement d'un élément de biométrie, l'information doit être immédiatement répliquée vers la base de données du serveur de biométrie.

BIOGDA03 : Fonctionnement autonome des lecteurs



Les bornes de lecture biométrique doivent pouvoir fonctionner de façon autonome en cas de dysfonctionnement réseau, en disposant d'une copie des informations permettant l'identification.

Une synchronisation entre les bases des lecteurs et celle du serveur doit se faire au minimum une fois par jour.

2.5.5 Gestion de l'exploitation et de la maintenance

BIOEXP01 : Recherche d'événements sur le système de gestion des accès



Le système de gestion d'accès doit permettre à minima de :

- réaliser des recherches multicritères sur l'historique ;
- permettre de retracer l'ensemble des accès tentés par les utilisateurs, succès et échecs.

2.6 Détection périmétrique

2.6.1 Introduction

La sûreté du centre pénitentiaire est assurée essentiellement par des dispositions de sûreté passive, constituées par des dispositifs constructifs (clôtures, barreaudages, vitrages antieffraction, etc.).

Elle est complétée par les systèmes de sûreté active suivantes :

- détection en zone neutre ;
- détection entrée chemin de ronde ;
- détection cour de service, cour du greffe et cour d'honneur ;
- détection en abord mur d'enceinte ;
- détection sur les toitures
- détection sur le glacis
- etc.

La liste ci-dessus n'est pas exhaustive, tout élément de détection périmétrique du domaine pénitentiaire est compris dans les présentes exigences.

Le type de détection est différent suivant la zone à surveiller, ci-dessous un exemple de dispositif de détection :

- détection par caméra thermique ;
- détection par barrière infra rouge ;
- éléments de détection sur les clôtures ;

2.6.2 Sécurité physique ou environnementale

PERPHY01 : Protection des dispositifs contre les attaques électromagnétiques		
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Les dispositifs en extérieur doivent être protégés contre les attaques électromagnétiques.		

2.7 Gestion des clés

2.7.1 Introduction

Ce système doit permettre aux établissements de faciliter la gestion des trousseaux de clés pour le personnel de l'établissement, grâce à une authentification par badge et biométrie.

Le système de gestion des clés peut être divisé en trois parties :

- le serveur applicatif contenant la base de données des accès autorisés ;
- la plateforme de gestion, constituée de :
 - l'UTL servant à la gestion de l'armoire à clef ;
 - le poste de travail de gestion permettant d'attribuer les droits sur les différents trousseaux de l'établissement.
- l'armoire :
 - les armoires à clés ;
 - les systèmes d'authentification de l'armoire.

2.7.2 Contrôle d'accès

CLEGDA01 : Authentification multi-facteurs



L'accès aux systèmes de gestion des clés doit être réalisé via une authentification multi-facteurs.

2.7.3 Gestion de l'exploitation et de la maintenance

CLEEXP01 : Journalisation des événements liés à l'ouverture de l'armoire à clés



Le système doit retracer les ouvertures réalisées par les différents utilisateurs (même sans prise de clé), ainsi que les clés retirées et rendues le cas échéant.