

SECRÉTARIAT GÉNÉRAL DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ SUD-OUEST
SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION DU MINISTÈRE DE L'INTÉRIEUR
SUD-OUEST
DIRECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION
CELLULE ZONALE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Site de la Préfecture de Tulle (19)

Cahier des Clauses Techniques Particulières.

Renouvellement d'une solution de contrôle d'accès et de vidéoprotection.

Référence du CCTP	SGAMI SO/ DSIC / CZSB / PREF_19 / 2026
Rédacteurs	DEWAELE Mathieu
Responsables techniques	-
Adresse	89 cours Dupré de Saint Maur 33000 Bordeaux
Téléphone	05 57 19 42 30 / 06 80 75 93 98
Email	-@interieur.gouv.fr
Date d'émission du cahier des charges	01/07/2026
Version	1
Pièces jointes	DPGF, Annexes

Table des matières

1 DESCRIPTION GÉNÉRALE DU PROJET.....	7
1.1 OBJET DE LA CONSULTATION.....	7
1.2 DESCRIPTION BATIMENTAIRE.....	7
2 PRINCIPE SYNTHÉTIQUE POUR LA CRÉATION D'UN SI DE SÛRETÉ DU MINISTÈRE.....	9
2.1 PROGRAMMATION DES COMMUTATEURS.....	11
2.2 PRÉSENCE DE PARE-FEUX.....	11
2.3 DIAGRAMME DES FLUX.....	13
2.4 PRINCIPE RETENU.....	14
3 PRESTATIONS ATTENDUES POUR LA PRÉFECTURE DE TULLE.....	16
3.1 BAIE ET COFFRET SÛRETÉ.....	16
3.2 INFRASTRUCTURE ET SERVEURS.....	16
3.3 VIDEOPROTECTION.....	17
3.4 CONTRÔLE D'ACCÈS.....	18
3.5 VISIOPHONIE.....	19
3.6 ASSERVISSEMENT DES SYSTÈMES DE SÛRETÉ.....	19
3.7 FORMATIONS.....	19
3.8 MAINTIEN EN CONDITION OPÉRATIONNELLE ET DE SÉCURITÉ.....	19
4 PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES (PSE).....	20
4.1 PSE n°1 ACTIVATION DES SERVICES RADIUS.....	20
4.2 PSE n°2 NAS SAUVEGARDE DES MACHINES VIRTUELLES.....	20
4.3 PSE n°3 INTRUSION CONCIERGERIE (COFFRET).....	20
4.4 PSE n°4 INTRUSION CONCIERGERIE (ACCUEIL PUBLIC).....	21
5 DESCRIPTIONS DÉTAILLÉES - LES BAIES ET LES COFFRETS DE SÛRETÉ.....	22
5.1 LA BAIE SÛRETÉ PRINCIPALE.....	22
5.2 LA BAIE SÛRETÉ SECONDAIRE (À REMPLACER).....	22
5.3 UN COFFRET SÛRETÉ (A CRÉER).....	22

6 DESCRIPTIONS DÉTAILLÉES - INFRASTRUCTURE ET SERVEURS.....	24
6.1 INFRASTRUCTURE RÉSEAU.....	24
6.1.1 LA ROCADE OPTIQUE.....	24
6.1.2 LA MATRICE DE FLUX.....	24
6.1.3 LES ÉLÉMENTS ACTIFS EXISTANTS.....	24
6.1.4 LES ÉLÉMENTS ACTIFS DISPONIBLE.....	25
6.1.5 ÉNERGIE.....	26
6.2 LES SERVEURS.....	27
6.2.1 SOLUTION INTRUSION (ET DE CONTRÔLE D'ACCÈS) HÉBERGÉE SUR SERVEUR.....	27
6.2.2 SERVEUR PRINCIPAL.....	27
6.2.3 SERVEUR REDONDANT.....	27
6.2.4 COMMUTATEURS/CONSOLE KVM.....	28
6.2.5 ONDULEURS.....	28
6.2.6 CARACTÉRISTIQUES TECHNIQUES DES SERVEURS.....	28
6.3 LES LICENCES ET MACHINES VIRTUELLES (VM).....	29
7 DESCRIPTIONS DÉTAILLÉES - VIDÉOPROTECTION.....	31
7.1 DESCRIPTION DU SYSTÈME VIDÉO EXISTANT.....	31
7.2 DESCRIPTION DÉTAILLÉE DES PRESTATIONS À RÉALISER.....	32
7.2.1 STOCKAGE DES FLUX VIDEOS.....	32
7.2.2 LES LICENCES VMS.....	32
7.2.3 LES POSTES DE VISUALISATION, D'EXPLOITATION ET D'EXTRACTION.....	33
7.2.3.1 POSTE DE RENVOIE D'IMAGES DE L'HÔTEL DE POLICE.....	33
7.2.3.2 LES FONCTIONNALITÉS ATTENDUES.....	34
7.2.4 LES POSTES À FOURNIR.....	34
7.2.4.1 POSTES DE VISUALISATION (qté 3).....	34
7.2.4.2 POSTE D'EXPLOITATION VIDÉO (qté 3).....	35
7.2.4.3 POSTE D'EXPORTATION VIDÉO	35
7.2.4.4 ÉCRAN 40/42 " SUR POSTE DÉJÀ EXISTANT (Qté 1).....	35
7.2.4.5 CARACTÉRISTIQUES TECHNIQUES DES POSTES.....	35
7.2.5 LES CAMERAS.....	36
8 DESCRIPTIONS DÉTAILLÉES - CONTRÔLE D'ACCÈS.....	39
8.1 CONTRÔLE D'ACCÈS EXISTANT ET LE GAC DISPONIBLE.....	39
8.2 LES ACCÈS CONTRÔLÉS.....	40

8.3 LES UNITÉS DE TRAITEMENT LOCAL (UTL).....	41
8.4 LES UNITÉS DE TRAITEMENT DE PORTE (UTP).....	42
8.5 LES LECTEURS DE BADGES (LB).....	42
8.6 ÉQUIPEMENTS DE PORTES.....	43
8.7 LA DÉTECTION INTRUSION EXISTANTE (HORS LOT).....	45
8.8 LES POSTES D'EXPLOITATION ET D'ENCODAGE.....	45
8.9 LES BADGES.....	46
9 DESCRIPTIONS DÉTAILLÉES - VISIOPHONIE.....	47
9.1 DESCRIPTION DE L'EXISTANT.....	47
9.2 DESCRIPTION DÉTAILLÉE DES PRESTATIONS À RÉALISER.....	47
9.3 DESCRIPTION TECHNIQUE.....	48
10 INTERFONCTIONNEMENT DES SYSTÈMES.....	50
11 LA CYBERSÉCURITÉ.....	51
12 COURANT FAIBLE, COURANT FORT, ÉTIQUETAGE.....	54
12.1 POINT PARTICULIERS A NOTER.....	54
12.2 COURANT FAIBLE.....	54
12.3 CAPILLAIRE CUIVRE.....	54
12.4 COURANT FORT ET ONDULEURS.....	55
12.5 ÉTIQUETAGE.....	56
12.6 ACTEUR.....	56
13 LA MAQUETTE.....	57
14 EXPLOITATION DE LA SOLUTION.....	58
14.1 GESTION DU SYSTÈME.....	58
14.2 EXPLOITATION PAR L'ADMINISTRATEUR DU SYSTÈME.....	59
14.2.1 CONFIGURATION DES DROITS OPÉRATEURS.....	59
14.2.2 GESTION DES JOURNAUX.....	61
14.3 EXPLOITATION PAR LES OPÉRATEURS.....	62
14.3.1.1 AMÉNAGEMENT DU POSTE DE GESTION.....	62

14.3.1.2 GESTION DES ENQUÊTES.....	62
14.3.1.3 GESTION DE LA CARTOGRAPHIE.....	63
14.3.1.4 GESTION DES ALARMES.....	64
14.3.1.5 GESTION DU SYSTÈME VIDÉO ET SCENARIOS.....	64
14.3.2 PRINCIPE DE GESTION DES RÉACTIONS A ÉVÉNEMENT.....	66
15 EXIGENCES SÉCURITAIRES.....	68
16 DÉPOSE ET REMPLACEMENT DES ÉQUIPEMENTS.....	72
16.1 DÉPOSE.....	72
16.2 STOCKAGE.....	72
16.3 RECYCLAGE.....	73
17 EXEMPLES DES ATTENDUS.....	74
17.1 EXEMPLE D'UN DIAGRAMME ET d'UNE MATRICE DE FLUX.....	74
17.2 PROPOSITION DE PLAN D'UNE ANALYSE FONCTIONNELLE D'UNE SOLUTION DE SÛRETÉ BATIMENTAIRE.....	77
17.3 EXEMPLES DE SCENARIOS D'ASSERVISSEMENTS.....	79
17.4 IMPLANTATION TYPE BAIE DU RÉPARTITEUR ET/OU SOUS-REPARTITEUR....	80
18 DOCUMENTATION.....	82
18.1 DOCUMENTATION TECHNIQUE.....	82
18.2 DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION.....	82
18.3 SAUVEGARDE ET RESTAURATION.....	82
19 FORMATION.....	84
20 RECETTE.....	85
20.1 RECETTE DE L'INFRASTRUCTURE RÉSEAU.....	85
20.1.1 LE CONTRÔLE VISUEL.....	85
20.1.2 LE CONTRÔLE FONCTIONNEL.....	86
20.1.2.1 TESTS DES LIAISONS CUIVRE.....	86
20.1.2.2 TESTS DES LIAISONS OPTIQUES.....	87
20.2 RECETTE DU COURANT FORT.....	88
20.2.1 LE CONTRÔLE VISUEL.....	88
20.2.2 LE CONTRÔLE FONCTIONNEL.....	88

20.3 RECETTE DES DIFFÉRENTS SYSTÈMES.....	88
20.3.1 LE CONTRÔLE QUANTITATIF ET QUALITATIF.....	89
20.3.2 LE CONTRÔLE FONCTIONNEL.....	89
20.4 PROCESS VERBAL DE RECETTE.....	90
20.5 LES FICHES DE RECETTE.....	90
20.6 VABF.....	90
20.7 VSR.....	91
20.8 RÉCEPTION DÉFINITIVE.....	92
21 GARANTIE.....	93
21.1 MODALITÉS.....	93
21.2 INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE.....	93
21.2.1 DÉFINITION DE LA GRAVITE DE L'INCIDENT.....	93
21.2.2 GARANTIES DE TEMPS DE RÉTABLISSEMENT (GTR).....	94
21.3 MISES A JOUR.....	94
21.4 INTERVENTION APRÈS LA PÉRIODE DE GARANTIE.....	94
22 PLANS.....	95
23 SYNOPTIQUES DU PROJET.....	96
24 DÉCOMPOSITION DU PRIX GLOBAL ET FORFAITAIRE.....	97
25 ANNEXES.....	98
25.1 ANNEXE 1 : PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT.....	98
25.2 ANNEXE 2 : PRINCIPE CONTRÔLE D'ACCÈS.....	98
25.3 ANNEXE 3 : NORMES ET RÉGLEMENTATIONS.....	98
25.4 ANNEXE 5 : PRINCIPE D'EXPLOITATION.....	98
25.5 ANNEXE 6 : PRINCIPE VIDÉOPROTECTION.....	98
26 GLOSSAIRE.....	99

1 DESCRIPTION GÉNÉRALE DU PROJET

1.1 OBJET DE LA CONSULTATION

Le présent document décrit les prestations à exécuter, fixe les règles d'ingénierie et les spécifications techniques à respecter ainsi que les composants à mettre en œuvre, pour la mise en sûreté.

ATTENTION !

Les annexes ci-après et celles fournies en pièces jointes font partie intégrante de ce CCTP.

À ce titre, leurs prescriptions sont à appliquer, en fonction du périmètre de la prestation demandée, aussi bien pour l'établissement de la proposition financière et technique,
que lors de la réalisation des travaux.

1.2 DESCRIPTION BATIMENTAIRE

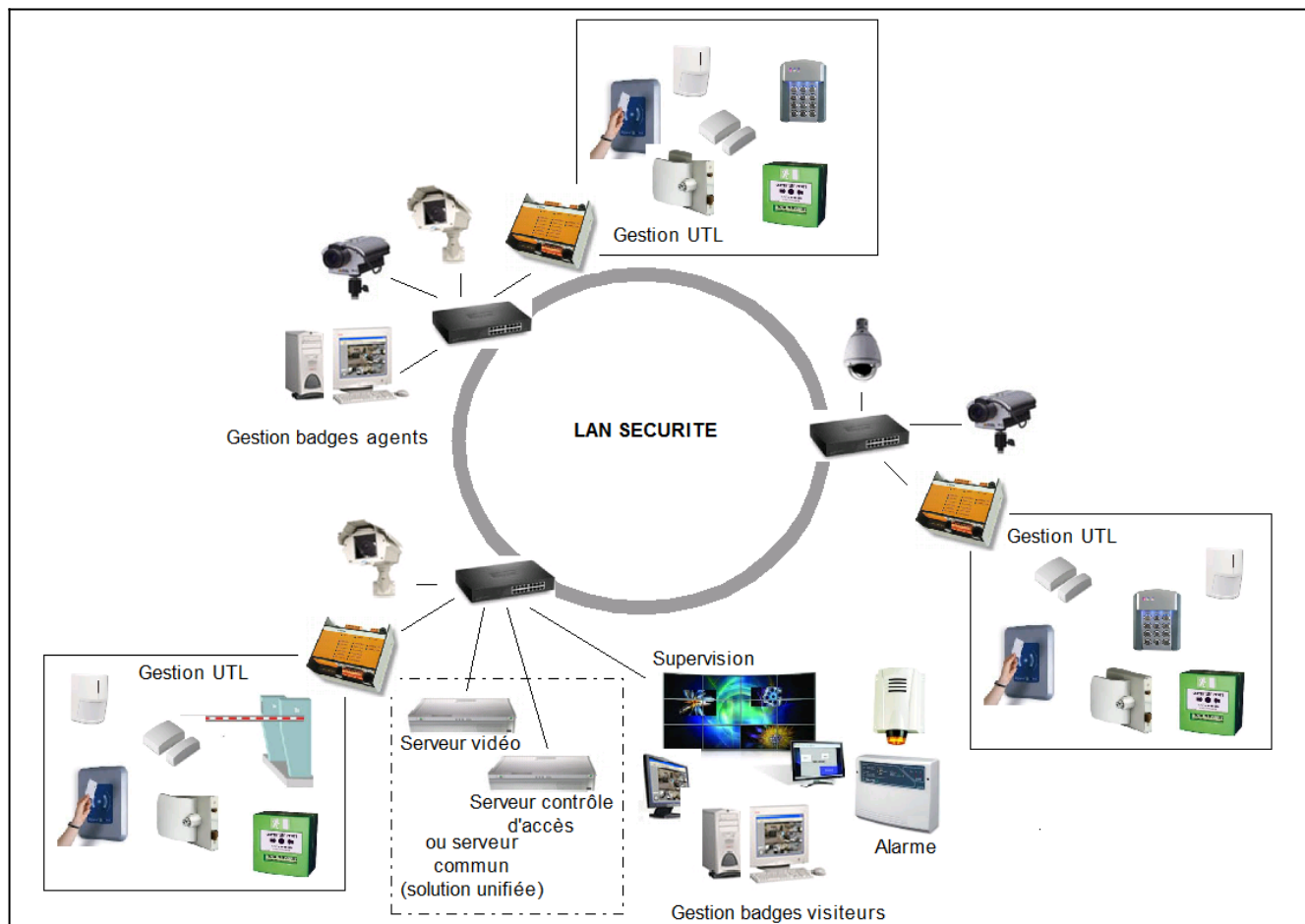
Le présent document décrit les prestations à exécuter, fixe les règles d'ingénierie et les spécifications techniques à respecter ainsi que les composants à mettre en œuvre, pour la mise en sûreté du site suivant :

La préfecture de Tulle est la Préfecture de Corrèze est implantée dans un secteur géographique délimité par :

- au Nord, une partie de la rue Marcelle Tinayre et la rue Pièce Verdier
- à l'Est, la rue Souham
- au Sud la place Roosevelt ainsi que des habitations (pavillons) desservies par la rue du Fouret
- à l'Ouest, la rue du Fouret et une partie de la rue Marcelle Tinayre



2 PRINCIPE SYNTHÉTIQUE POUR LA CRÉATION D'UN SI DE SÛRETÉ DU MINISTÈRE



Le système est prévu pour apporter une solution de sécurité unifiée et ouverte en assurant la préservation des biens et des personnes, un renforcement de la protection des biens contre tout acte de vandalisme, contre les dégradations et contre toute agression.

Toutes les liaisons entre les éléments du réseau sûreté (commutateurs, serveurs, stations, caméras) seront filaires.

Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.

Le réseau Ethernet Sûreté sera destiné à accueillir les applications suivantes :

- Vidéosurveillance,
- Contrôle d'accès,

- Détection d'intrusion.

Le LAN sûreté physique sera constitué d'un commutateur Ethernet qui sera le cœur de concentration.

Le commutateur est de type distribution (équipé de ports SFP-1000Base-X), et « POE ».

Ce commutateur possède plusieurs ports 1000baseT pour le raccordement des périphériques critiques (serveur, station d'affichage ou autre).

Le commutateur servira de référence pour tous les raccordements de périphériques « Ethernet-IP ».

Il disposera d'un nombre suffisant d'interfaces gigabits pour supporter les équipements qui y seront raccordés.

Une réserve de 10% d'interfaces de chaque type sera prévue pour une éventuelle extension.

Les règles de sécurité définies par le Haut Fonctionnaire de Défense (HFD/RCSSI) imposent une étanchéité stricte entre les flux vidéo extérieurs et le reste du Système d'Information de Sûreté (SIS).

Afin d'assurer l'homogénéité du réseau et la compatibilité avec les composants actifs en service sur le site, les commutateurs Ethernet et pare-feu utilisés dans la solution figureront au catalogue des solutions informatique du Ministère de l'Intérieur.

Cette contrainte s'explique par l'obligation de respecter sur tous les sites du Ministère de l'Intérieur des préconisations d'architectures réseau précises et strictes, et basées sur des matériels validés pour leur aptitude à répondre à ces besoins.

Le respect de ces préconisations en particulier du point de vue des éléments actifs, est que le prérequis incontournable à l'intégration du réseau de protection objet du présent marché, au réseau local du site.

Les commutateurs des séries HP 5140, HP 5520 (utilisation en niveau 2-accès) sont conformes et déployés actuellement par le Ministère de l'Intérieur.

Les commutateurs seront fournis par l'administration, configurés et installés en collaboration avec les techniciens du ministère de l'Intérieur.

2.1 PROGRAMMATION DES COMMUTATEURS

Le soumissionnaire devra fournir à l'issue de l'installation :

- Le plan d'adressage IP
- Les protocoles mis en œuvre
- Les ports (origine et destination)
- Les fichiers TXT de chaque commutateur sous format électronique (*.Txt)
- Les remarques éventuelles

Le LAN sûreté sera constitué d'autant de réseaux virtuels (VLANs) qu'il y aura de types de matériels installés. Les commutateurs Ethernet seront configurés par les techniciens du ministère en collaboration avec les techniciens du soumissionnaire.

Dans ce CCTP le contrôle d'accès et la vidéoprotection sont abordés. En conséquence les VLANs de ces métiers sont demandés dans la bulle sûreté.

Pour le contrôle d'accès et l'anti-intrusion, les VLANs suivants sont ou seront créés :

- pour l'administration de contrôle d'accès,
- pour le serveur de contrôle d'accès,
- pour les UTL,
- pour les autres équipements éventuels.
- pour les alarmes

Pour la vidéosurveillance les VLANs suivants seront créés :

- pour l'administration et la supervision vidéo,
- pour la gestion et l'enregistrement des images,
- pour les caméras intérieures,
- pour les caméras extérieures,
- pour la visiophonie.

Le commutateur n'assurera en aucun cas le routage inter Vlan.

2.2 PRÉSENCE DE PARE-FEUX

La fonction de routage inter Vlan sera exclusivement assurée par un pare-feu de niveau 3 qui aura la double fonction de filtrage et de routage des Vlan.

Les pare-feux du réseau Ethernet Sûreté sont conformes aux préconisations du Ministère de l'Intérieur.

Ceux déployés actuellement par le Ministère de l'Intérieur sont de séries FORTINET Fortigate 60D/100D/200D/300D.

Le pare-feu nécessaire à ce projet est fourni par l'administration, configuré et installé en collaboration entre les techniciens du ministère de l'Intérieur et ceux du soumissionnaire.

Au début de la phase de réalisation, l'intégrateur fournira les informations nécessaires et complets à l'établissement de la matrice de flux conforme au site et s'appuyant sur l'exemple pour une solution de contrôle d'accès et de vidéosurveillance. L'intégrateur fournira obligatoirement au ministère cette matrice de flux pour chacun des sites concernés par la solution.

Cette base servira à l'administration qui se chargera de la configuration des pare-feux.

Ces informations comprendront notamment :

- Les adresses IP source et destination,
- Les flux source et destination,
- Les ports origine et destination,
- Les protocoles,
- Les débits,
- Les fréquences (flux permanent ou ponctuel),
- Les remarques éventuelles,
- Tout paramétrage autorisé pour assurer le fonctionnement sécurisé de la solution.

Le soumissionnaire présentera ces renseignements dans le tableau joint en annexe dont l'administration lui communiquera une version électronique.

Compte tenu du délai de deux mois nécessaire à l'administration au traitement de ces informations pour leur mise en forme et à l'intégration dans une base de données nationale, la mise en réseau de la solution de sûreté bâtimementaire, objet du présent CCTP, ne pourra pas intervenir avant l'issue de ces deux mois. Le soumissionnaire tiendra compte de ce délai et l'intégrera dans le calendrier de déploiement de la solution qu'il proposera.

Le réseau de sûreté est ou devra être indépendant du réseau existant du site.

2.3 DIAGRAMME DES FLUX

Un Diagramme de Flux réseaux représente schématiquement l'ensemble des flux entre chaque équipement du réseau qui le compose. Il a pour but d'indiquer de façon claire et précise les protocoles, numéros de port ainsi que son mode de fonctionnement (connecté et/ou non connecté).

Le sens des flèches définit la direction du flux. Il doit également représenter le sens du trafic. Il convient également de modéliser les sous-réseaux qui le compose.

Ce diagramme permettra à l'intégrateur de construire la matrice de flux nécessaire à la configuration du pare-feu du site. L'intégrateur fournira obligatoirement au ministère cette matrice de flux pour chacun des sites concernés par la solution.

Tout ce qui n'est pas déclaré dans le diagramme et la matrice de flux ne sera pas pris en compte.

Le soumissionnaire devra inclure dans son offre technique une ébauche de la matrice et du diagramme de flux du projet.

Vous trouverez un exemple de diagramme et d'une matrice de flux pour une solution de vidéosurveillance au §17.1 page 74. Le soumissionnaire effectuera, si besoin, le même traitement pour les métiers du contrôle d'accès et de l'anti-intrusion.

2.4 PRINCIPE RETENU

L'objet de ce CCTP porte sur :

- La fourniture, le remplacement, l'installation, le raccordement et la mise en service d'un système de contrôle d'accès (câblage courants forts et faibles, éléments matériels actifs, passifs et logiciels).
- La fourniture, le remplacement, l'installation, le raccordement et la mise en service d'un système de vidéoprotection (câblage courants forts et faibles, éléments matériels actifs, passifs et logiciels).
- La dépose, stockage et/ou enlèvement du matériel obsolète.
- Le remplacement, la dépollution du câblage existant de contrôle d'accès intérieure et extérieure.
- Le remplacement, la dépollution du câblage existant de vidéoprotection intérieure et extérieure.
- La fourniture de la documentation détaillée.
- La formation des personnels chargés de la gestion et l'exploitation du système mis en œuvre.
- La garantie sur le matériel et les logiciels comprenant la maintenance préventive, corrective, évolutive et adaptative du contrôle d'accès et de la vidéoprotection (architecture technique, logiciels) livrés.

La prestation devra respecter les mesures de sécurité (cf.§15 p68) et la réglementation en vigueur (cf. §25.5 p98).

Les plans et documents nécessaires à l'élaboration du projet seront remis par l'administration ou son représentant lors de la visite de site.

Les fonds de plans au format « dwg ou pdf » seront remis au titulaire du marché pour mise à jour et confection du DOE à fournir dans le cadre de la recette (cf. §20 p85). La version logicielle sera à définir pour une lecture aisée des documents.

Le soumissionnaire devra fournir, dans le dossier technique présenté dans son offre, toute certification ou agrément délivré par les constructeurs des matériels ou logiciels constituant son offre technique.

Qualifications requises ou équivalentes (à préciser):

- APSAD R81, R82, D83, ou équivalent ;

- Preuve de partenariat avec éditeur / constructeur sûreté disposant certification / qualification suivant dernier référentiel ANSSI à jour;
- ISO 27001 ou équivalent;

Autres :

- Justification des références sur des projets de mise en sûreté similaires pour opérateurs étatiques (3 dernières années)
- Justification d'une preuve d'une représentation locale;
- Justification d'un centre d'intégration qui lui est propre pour un maquettage à l'échelle 1;
- Justification de l'existence d'un centre de veille des vulnérabilités (CERT : Computer Emergency Response Team).

3 PRESTATIONS ATTENDUES POUR LA PRÉFECTURE DE TULLE

Le présent marché a pour objet la mise à jour complète des systèmes de contrôle d'accès, de la visiophonie et de vidéoprotection destinées à protéger certains ouvrants, les lieux de travail et les locaux sensibles.

3.1 BAIE ET COFFRET SÛRETÉ

Fourniture et installation

- Remplacer la baie existante 42U 800x800 par une baie serveur de 42U 800x1000 à fournir et installer (COD) avec l'aide de l'administration pour le raccordement électrique et la réinstallation du réseau. Pas besoin de prévoir d'accessoires complémentaires
- Installer baie murale à la conciergerie et la raccorder électriquement et fourniture des accessoires. Ramener la fibre OM 4 multimodes (12 brins minimum) jusqu'à cette baie depuis le SR du bâtiment principal. (Un switch sûreté y sera installé et configuré par l'administration.)

3.2 INFRASTRUCTURE ET SERVEURS

Fourniture

- Fourniture de la licence de redondance haute disponibilité Safekit ou équivalent

Installation

- Installation de 1 KVM avec clavier et écran LCD, un dans la baie serveur redondante de sûreté.
- Installation et programmation de 1 onduleur avec carte SNMP pour le serveur de sûreté redondant.

Maquette

- Maquettage sur site

Fourniture, Mise en Service et Programmation

- Fourniture et création des licences pour les VM nécessaires au projet sur le serveur principal
- Mise en service du serveur pour la redondance avec fourniture des licences nécessaire à la création des VM.
- Fournir et programmer la licence de redondance haute disponibilité (des Machines Virtuelles) entre les 2 serveurs.

3.3 VIDEOPROTECTION

L'intégrateur devra prévoir des équipements de levage (nacelle) adaptés à la topographie de la rue (déclivité importante).

Câblage (Remplacement)

- Refonte du câblage (Dépose, dépollution et tirage de nouveaux câbles)

Dépose et/ou remplacement

- Dépose : 3x caméras intérieur & alimentations
- Dépose : 6x caméras extérieur & alimentations

Fourniture, installation, mise en service et programmation

- Dimensionner et fournir les disques durs de stockage des flux vidéo nécessaires (serveur principal et serveur redondant). Ce dimensionnement devra être justifié par une note de calcul détaillée.
- 10 x Caméras en intérieur (dont 1 ISIS)
- 16x Caméras extérieur à installer (13 Bullet, 2 mini-dôme, 1x 180°)
- Tout accessoire nécessaire à l'installation des caméras et des moniteurs selon leur type et position.
- 1x Poste d'exploitation Vidéo - COD sans écran (fourniture 1x écran 27" par la préfecture)
- 1x Poste d'exploitation Vidéo – Commissariat de Tulle sans écran (fourniture 1x écran 27" par la préfecture)
- 1x Poste d'exploitation Vidéo – SIDSIC sans écran (fourniture 1x écran 27" par la préfecture)
- 1x Poste de visualisation Vidéo – Accueil sans écran (fourniture 1x écran 27" par la préfecture)

- 1x Poste de visualisation Vidéo – Préfet sans écran (fourniture 1x écran 27" par la préfecture)
- 1x Poste de visualisation Vidéo – Standard avec fourniture et pose 1 écran 40/42" et support mural
- Fourniture et pose 1 écran 40/42" et support mural sur le Poste d'exploitation Intrusion – DDS (poste déjà existant)
- Tous câbles IP, **en intérieur comme en extérieur**, le cas échéant analogique existants, devront être remplacés par des liaisons IP conformes aux exigences de performance et de sécurité. Ses nouveaux câbles IP devront être pourvus de protections adéquates, qui plus est, avec la mise en place de protection physique de type oméga métallique pour les passages en extérieur.
- Dans le cadre des travaux, il conviendra de procéder au retrait des anciens câbles, dans la mesure où cela est réalisable.
- Procéder à la dépollution et à la mise hors service des alimentations des caméras déposées.
- Réaliser l'ensemble des tirages de câbles nécessaires au fonctionnement complet et cohérent du système.

3.4 CONTRÔLE D'ACCÈS

Câblage (Remplacement)

- Refonte du câblage (Dépose, dépollution des câbles lecteurs et câbles des équipements de verrouillage avec tirage de nouveaux câbles)

Fourniture, installation et mise en service pour création complète

- Création de 5 lecteurs de badge, avec verrouillage et environnement de porte et ferme porte à fournir et installer.

Fourniture, et remplacement

- Remplacement de 30 lecteurs de badges
- Prévoir le remplacement de l'ensemble des batteries des coffrets d'alimentation de verrouillage des portes et/ou remplacement intégral des coffrets de verrouillage.

Fourniture, licence et programmation

- 1x Licence pour le poste d'exploitation intrusion existant - bureau DDS/SIDSIC ? + lecteur encodeur de badge usb)

3.5 VISIOPHONIE

Câblage (Remplacement)

- Refonte du câblage (Dépose, dépollution et tirage de nouveaux câbles)

Fourniture, installation, mise en service et programmation

- 1x poste de Réception Écran 7 " ou équivalent – Accueil
- 1x poste de Réception Écran 7 " ou équivalent – Résidence du préfet
- 1x poste de Réception Écran 7 " ou équivalent – Standard
- 1x Visiophone 2BP – Entrée Principale public
- 1x Visiophone 2BP – Portail d'honneur
- 1x Visiophone 2BP – Portail Parking et Barrière

3.6 ASSERVISSEMENT DES SYSTÈMES DE SÛRETÉ

- Prévoir, réaliser, et paramétrer en fonction d'une analyse fonctionnelle, des asservissements entre les systèmes de contrôle d'accès, la visiophonie, de vidéosurveillance et de l'intrusion.

3.7 FORMATIONS

- Réaliser des formations utilisateurs et administrateurs pour l'ensemble de la solution.

3.8 MAINTIEN EN CONDITION OPÉRATIONNELLE ET DE SÉCURITÉ

- Proposer une offre de contrat de maintenance pour assurer les MCO/MCS de la solution (contrat prêt à être signé).

4 PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES (PSE)

4.1 PSE N°1 ACTIVATION DES SERVICES RADIUS

Le soumissionnaire fournira les certificats et mettra en place les services radius sur l'ensemble des périphériques IP tels que décrit dans le CCTP.

Le soumissionnaire devra assurer le paramétrage des certificats RADIUS nécessaires au fonctionnement du service.

4.2 PSE N°2 NAS SAUVEGARDE DES MACHINES VIRTUELLES

Demandé en Prestation Supplémentaire Éventuelle (PSE), un serveur NAS sera à mettre en œuvre, afin d'assurer la sauvegarde des machines virtuelles. Le dimensionnement du NAS est basé sur une sauvegarde journalière/hebdomadaire/mensuelle et incrémentielle de l'intégralité du système avec une conservation des 15 copies consécutives. De plus chaque sauvegarde est chiffrée et résiliente aux attaques par ransomware.

4.3 PSE N°3 INTRUSION CONCIERGERIE (COFFRET)

Demandé en Prestation Supplémentaire Éventuelle (PSE), le soumissionnaire fournira et mettra en place une détection intrusion dans la conciergerie dans laquelle sera installé le nouveau coffret mural recevant le switch de sûreté. Cette détection intrusion sera composée à minima

- d'une UTL,
- d'une carte entrée relais UTR,
- avec son coffret d'alimentation secourue,
- un détecteur volumétrique NFA2P Type3
- deux contacts d'ouverture NFA2P Type3 à installer sur la porte double
- un contact d'ouverture préférence NFA2P Type3 à installer sur la porte du coffret mural
- un clavier de mise en/mise hors.

Le coffret d'alimentation secourue permettra de tenir pour tenir 72h en cas de coupure 230v. Le soumissionnaire fournira les calculs d'autonomie pour justifier de son choix de batterie.

4.4 PSE N°4 INTRUSION CONCIERGERIE (ACCUEIL PUBLIC)

Demandé en Prestation Supplémentaire Éventuelle (PSE), le soumissionnaire fournira et mettra en place une détection intrusion dans la conciergerie qui sera réhabilitée, destinée à accueillir le public en cas d'événements. La conciergerie (Coffret), visée par la PSE 3, sera considérée comme déjà équipée de l'UTL et de la carte relais. Cette dernière permettra le raccordement des points de détection et de commande énumérés ci-dessous. Pour assurer cette liaison, le soumissionnaire devra prévoir la réalisation d'une tranchée entre les deux conciergeries. En ce qui concerne les travaux de VRD, un fourreau existant sous le bitume permettra le passage sous le bitume seul des tranchées sur herbe seront à prévoir. Dans le cas contraire, les travaux de VRD sur bitume seront à prévoir également par le soumissionnaire.

Cette détection intrusion sera composée à minima :

- avec son coffret d'alimentation secourue,
- un détecteur volumétrique NFA2P Type3
- deux contacts d'ouverture NFA2P Type3 à installer sur la porte double
- un clavier de mise en/mise hors.

Le coffret d'alimentation secourue permettra de tenir pour tenir 72h en cas de coupure 230v. Le soumissionnaire fournira les calculs d'autonomie pour justifier de son choix de batterie.

5 DESCRIPTIONS DÉTAILLÉES - LES BAIES ET LES COFFRETS DE SÛRETÉ

5.1 LA BAIE SÛRETÉ PRINCIPALE

La baie serveur de sûreté de 800x1000 42U dans le local RG est complète et déjà installée. Cette baie héberge le serveur de sûreté principal.

5.2 LA BAIE SÛRETÉ SECONDAIRE (À REMPLACER)

Concernant le serveur redondant, lui sera à installer dans une baie située à l'étage du C.O.D. La baie actuellement en place est une baie de 800x800 42U. Elle n'est donc pas dimensionnée pour recevoir le serveur de redondance.

Elle est déjà raccordée électriquement et raccordée en points réseaux. Elle contient également déjà différents équipements (bandeau de brassage, passe câbles...).

Le candidat devra prévoir de remplacer cette baie par :

1 baie* 800x1000 42U (fourniture et pose à prévoir par le candidat) qui servira à y installer le serveur de redondance et son onduleur. L'administration s'occupera de faire la transition courant faible et courant fort de l'ancienne baie vers la nouvelle. En concordance avec le candidat pour la bonne mise en place de celle-ci.

**Baie serveur à fournir sans accessoires de types passe câbles, bandeau RJ, Fibre ...*

5.3 UN COFFRET SÛRETÉ (A CRÉER)

Concernant la conciergerie, il est quant à lui démunie d'équipements réseau et d'arrivée fibre optique, il a tout de même une arrivée électrique.

Le candidat devra prévoir dans son offre la fourniture, l'installation et le raccordement de ce coffret mural à la conciergerie.

Ce coffret devra être de un coffret de 800x600 6U qui contiendra uniquement un switch de sûreté, son tiroir optique et son bandeau de prises RJ45.

Le candidat devra également tirer l'arrivée du réseau sûreté par fibre optique, OM 4 multimodes de 12 brins minimum prévue pour passage en extérieur, depuis le bâtiment principal dans les règles de l'art. (Ex : Protection oméga métallique si passage en extérieur, ...)

Le candidat devra également prévoir le raccordement électrique de ce coffret.

Remarques : Les baies sûretés (et coffrets) devront être complètes avec présence des joues latérales, fond, toit, sol, et serrures.

6 DESCRIPTIONS DÉTAILLÉES - INFRASTRUCTURE ET SERVEURS

6.1 INFRASTRUCTURE RÉSEAU

L'infrastructure réseau sera à réaliser conformément aux caractéristiques et aux principes décrits dans l'annexe du présent CCTP dénommée :

ANNEXE 1 : CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

Toutes les liaisons entre les éléments du réseau sûreté (lecteurs de badges, UTL, commutateurs, serveurs, stations, caméras) seront filaires. Aucun lien sans-fil ne sera admis, sauf spécification explicite contraire présente dans ce CCTP.

Les sites, la préfecture de Tulle, et l'Hôtel de Police, sont équipés de part-feu.

6.1.1 LA ROCADE OPTIQUE

Une liaison fibre optique point à point et dédiée entre les deux (futurs) baies de sûreté pour le serveur et le serveur redondant est existante et fonctionnelle sur le site de la Préfecture. Ce lien permet de réaliser le transfert des VM en Haute Disponibilité d'un serveur vers l'autre en cas d'indisponibilité ou d'arrêt de l'un des hôtes. Les autres liaisons entre les Sous-Répartiteurs sont également existants.

6.1.2 LA MATRICE DE FLUX

Conformément au chapitre 2 l'intégrateur fournira, par site, la matrice de flux nécessaire au bon fonctionnement de l'ensemble de la solution.

6.1.3 LES ÉLÉMENTS ACTIFS EXISTANTS

Un ou plusieurs commutateur-s en réseau local permettent, actuellement, la communication entre équipements vidéo et contrôle d'accès. (Ce-s dernier-s seront à déposer.) (Les caméras sont, pour la plupart, analogiques)

Le système de détection intrusion et le serveur principal sont quant à eux déjà raccordés à un switch sûreté derrière un pare-feu – « bulle sûreté ».

6.1.4 LES ÉLÉMENTS ACTIFS DISPONIBLE

Leur fourniture et mise en service sont exclues de la présente prestation.

L'administration a réalisé une estimation du nombre de commutateurs réseau à mettre en œuvre et les fournira, ainsi que le pare-feu nécessaire à l'établissement des liens sécurisés inter-sites.

Le Ministère de l'Intérieur fournira tous les éléments permettant la segmentation du réseau (Numéros de VLAN, adresses IP des LAN, masques de sous-réseaux, etc.) via son Bureau des Réseaux Fixes de la DSIC du SGAMI.

Pour information :

Le soumissionnaire dimensionnera précisément l'architecture du réseau de sûreté à mettre en place en se conformant au besoin décrit dans le CCTP et aux principes décrits dans l'annexe 1.

Il précisera le nombre exact de commutateurs nécessaires au déploiement de cette architecture en tenant compte du nombre et de l'emplacement des locaux techniques auxquels les périphériques (des trois métiers) de la solution de sûreté sont rattachés (contrainte du câblage sur les distances de raccordement)

Les commutateurs et pare-feux sont listés ci-après :

Répart. : Répartiteur où l'équipement sera installé

P : Pare-feu

C : Commutateur

SUR LE SITE DE LA PRÉFECTURE						
Bâti ment	Etage	Répart.	Fonction	P	C SFP	C PoE
	-	RG	Répartiteur Serveur Connexion des éléments sûreté (pare-feu, serveurs, commutateur)	1 ^{Existant}	1 ^{Existant}	1 ^{Existant}
	-	SR COD	SR Serveur Redondant			1
	-	SR RDC	SR RDC			1
	-	SR HP	SR Hôtel Préfectoral			1
	-	Conciergerie	SR Conciergerie (baie à créer)			1
Éléments actifs existants, quantités totales :				1 ^{Existant}	1 ^{Existant}	1 ^{Existant}
Éléments actifs à fournir et à installer par l'administration, quantités totales :						4

SUR LE SITE DE L'HÔTEL DE POLICE						
Bâti ment	Etage	Répart.	Fonction	P	C SFP	C PoE
		...	Répartiteur Connexion des éléments sûreté (pare-feu, commutateur)	1 ^{Existant}		1 ^{Existant}
Éléments actifs existants, quantités totales :				1 ^{Existant}		1 ^{Existant}
Éléments actifs à fournir et à installer par l'administration, quantités totales :				0		0

*1 pare-feu fortinet type 60 ou 200D

*SFP : switchs SFP HP 5520

*PoE : switchs POE HP 5140

6.1.5 ÉNERGIE

Les locaux techniques cités sont alimentés par le réseau ondulé 230V lui-même raccordé sur le groupe électrogène du site.

6.2 LES SERVEURS

6.2.1 SOLUTION INTRUSION (ET DE CONTRÔLE D'ACCÈS) HÉBERGÉE SUR SERVEUR

La solution de détection d'intrusion déployée à la préfecture de Tulle, dans le cadre de l'exercice budgétaire précédent, repose sur une plateforme commune intégrant à la fois la détection d'intrusion et le contrôle d'accès.

Elle est composée d'équipements de la gamme XSECUR'-EVO de SYNCHRONIC qui devra assurer également la gestion centralisée (G.A.C.) de la solution de contrôle d'accès à construire.

6.2.2 SERVEUR PRINCIPAL

Le serveur principal fait partie du matériel déjà opérationnel installé dans le RG. Il héberge actuellement

- la machine virtuelle pour l'Active Directory
- et la machine virtuelle pour le GAC de détection intrusion (solution commune au contrôle d'accès)

Il est le serveur dans lequel le candidat devra créer et incrémenter en Machine Virtuelle (VM) le rôle de la vidéoprotection et le rôle du radius :

- Gestion de la vidéo et Enregistrement des flux vidéos.
- Serveur associé aux rôles de la cybersécurité dont le Radius

En cas de dysfonctionnement, ce serveur principal est secouru par le serveur de redondance.

Le candidat devra dimensionner et configurer les ressources nécessaires au bon fonctionnement des machines virtuelles (CPU, mémoire, stockage).

6.2.3 SERVEUR REDONDANT

Le serveur redondant fait partie du matériel déjà livré. Il est actuellement allumé et branché électriquement.

Le candidat prévoira de paramétrer et de mettre en service la solution de redondance entre les 2 serveurs de sûreté. (fonctionnalités de redondance et des machines virtuelles. Les serveurs étant déjà achetés lors de l'exercice budgétaire précédent.)

Le serveur de redondance devra héberger de façon identique en machines virtuelles les mêmes types de rôles serveur. Il sera à installer dans une baie

distincte de celle du serveur principal, notamment dans la baie prévue à proximité de la salle C.O.D.

Le candidat devra dimensionner et configurer les ressources nécessaires au bon fonctionnement des machines virtuelles (CPU, mémoire, stockage).

La redondance haut débit du serveur principal sera assurée par le logiciel SafeKit d'Evidian ou un équivalent, permettant le basculement des machines virtuelles d'un serveur à l'autre.

Le titulaire devra fournir la licence correspondante et garantir le bon fonctionnement du mécanisme de basculement des machines virtuelles mises en œuvre dans le cadre du présent marché.

Durée d'enregistrement

Concernant le serveur de redondance en cas de défaillances du serveur principal, les caméras seront à enregistrer 24 heures sur 24, sur une durée de 08 jours glissants.

Le dimensionnement sera calculé en prenant en compte la résolution maximale de chaque caméra et de chaque visiophone.

Le soumissionnaire justifiera dans son offre le dimensionnement des disques durs par des calculs détaillés.

6.2.4 COMMUTATEURS/CONSOLE KVM

Le soumissionnaire prévoira d'installer pour la baie du serveur redondant un commutateur KVM LCD rackable 19" afin de pouvoir administrer le/les serveur.s. directement depuis le local technique sans passer par un poste d'exploitation.

Ce KVM LCD est déjà fourni suite à exercice budgétaire précédent et est toujours sous carton.

6.2.5 ONDULEURS

Le soumissionnaire prévoira d'installer pour la baie du serveur redondant l'onduleur déjà fourni suite à exercice budgétaire précédent et est toujours sous carton. Cf chapitre Courant Fort et Onduleurs.

6.2.6 CARACTÉRISTIQUES TECHNIQUES DES SERVEURS

Les serveurs livrés respectent à minima les critères suivants :

- Technologie « x86 64 bits »,
- Sans modification logicielle (e.g. BIOS) ou matérielle qui ne serait pas transposable sur tout autre serveur de même technologie,

- Rackables,
- Alimentation redondante,
- Produit par un des 5 premiers constructeurs mondiaux de serveurs généralistes en volume qui doit avoir noué des partenariats avec les principaux intégrateurs couvrant le territoire français (à justifier dans la réponse),
- Garantie 5 ans pièce et main d'œuvre

Les systèmes d'exploitation devront être la dernière version stable de Windows Serveur.
Une infrastructure virtualisée est en place en Microsoft Hyper-V.

Configuration technique minimale des serveurs :

- 2xCPU 16 cœurs (AMD ou Intel)
- RAM: 128Go minimum
- RAID1 SYSTEME de 256 Go mini en SSD
- 4 Ports Ethernet
- 1 Port minimum SFP Gb/s et son module Gbic
- Licence Windows server STD 2025 ou supérieur (permet de couvrir 2xCPU 16 cœurs + 2VMs)
- RAID5 n disques montés en Raid 5, (n sera précisé par l'intégrateur qui le justifiera en produisant la note de calcul permettant de dimensionner le serveur d'archivage vidéo)
- Standard, License & Media, VMs: 2 Licensed Cores: 16
- Kit rail de montage

Les serveurs, livrés dans le cadre d'un exercice budgétaire précédent, sont dépourvus de disque dur de stockage vidéo. C'est pour cela que le titulaire devra calculer la volumétrie des enregistrements engendrée par les caméras numériques posées au titre de la prestation. La volumétrie sera calculée en prenant en compte la résolution maximale de chaque caméra et des visiophones.

6.3 LES LICENCES ET MACHINES VIRTUELLES (VM)

Le candidat devra fournir l'ensemble des licences VM afin de créer les machines virtuelles nécessaires au bon fonctionnement de la solution

proposée à la foi pour le serveur principal et pour le serveur de redondance.

Le candidat devra réaliser la programmation du serveur principal pour héberger les solutions métiers de ce présent CCTP en machines virtuelles sous forme de VM :

- la VM pour la gestion de la vidéo-surveillance et le stockage des images (enregistrement),
- la VM pour la sécurisation des périphériques (RADIUS authentication 802.1x EAP-TLS), la gestion des utilisateurs et de l'exploitation (contrôleur de domaine & management système) si non existante au préalable.

Le titulaire fournira en phase chantier :

- les prérequis des équipements constitutifs de la solution garantissant le bon fonctionnement de la solution.
- une documentation d'installation détaillée de la solution ainsi que tous les paramètres de configuration et mots de passe.

7 DESCRIPTIONS DÉTAILLÉES - VIDÉOPROTECTION

ATTENTION !

L'installation du système de vidéo surveillance sera réalisée conformément aux principes décrits dans l'annexe à ce CCTP dénommée :

ANNEXE 6 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES VIDÉO PROTECTION 2024

Tout accès via internet et autres réseaux externes est formellement interdit, de même que les alertes par SMS

7.1 DESCRIPTION DU SYSTÈME VIDÉO EXISTANT

D'une part le système vidéo existant est composé d'un enregistreur vidéo. Le, les enregistreurs, les postes d'exploitation vidéo et les caméras sont raccordés sur un réseau local vidéo indépendant. Les caméras sont raccordées sur des switchs via PoE ou par câbles analogiques et câbles alimentations électriques.

D'autre part, la préfecture possède un serveur principal de sûreté (évoqué dans le paragraphe précédent §6.2.2 page 27 ainsi qu'un serveur redondant de sûreté suffisamment dimensionnés afin d'y intégrer ou de créer la Machine Virtuelle de Vidéosurveillance et la Machine Virtuelle Radius. (La redondance entre les deux serveurs s'effectuera grâce à la solution SafeKit ou équivalent.)

Cependant, ces deux serveurs sont dépourvus de disque dur de stockage vidéo. Ils seront donc à prévoir dans le cadre de ce projet.

L'Hôtel de Police de Tulle, dispose d'un renvoi de vidéosurveillance qui permet de visualiser les caméras de la préfecture.

La Préfecture dispose actuellement de caméras analogiques, voir IP, obsolètes.

La préfecture compte 9 caméras réparties comme suit :

- 6 en extérieur
- et 3 en intérieur

Ces caméras ne sont pas asservies au système de détection d'intrusion.

7.2 DESCRIPTION DÉTAILLÉE DES PRESTATIONS À RÉALISER

Les services de la préfecture souhaitent assurer la remise en état ou le remplacement des caméras défectueuses par des technologies adaptées, procéder au déplacement ou à la réimplantation des caméras en fonction des travaux.

Le candidat prévoira d'installer et configurer le logiciel de gestion vidéo (VMS) sous environnement virtualisé, conformément aux recommandations éditeur et aux bonnes pratiques d'architecture.

7.2.1 STOCKAGE DES FLUX VIDEOS

Le candidat devra fournir dans son offre les disques durs de stockage des flux vidéo pour le serveur principal tout comme pour le serveur de redondance.

Le candidat devra également prévoir dans son offre, l'enregistrement des flux vidéo des visiophones dans le serveur d'enregistrement au même type que les caméras.

La durée d'enregistrement

Toutes les images issues des visiophones et des caméras seront à enregistrer 24 heures sur 24, sur une durée de 30 jours glissants sur le serveur principal. Concernant le serveur de redondance en cas de défaillances du serveur principal, les caméras seront à enregistrer 24 heures sur 24, sur une durée de 08 jours glissants.

Le dimensionnement sera calculé en prenant en compte la résolution maximale de chaque caméra.

Le soumissionnaire justifiera dans son offre le dimensionnement des disques durs par des calculs détaillés.

7.2.2 LES LICENCES VMS

Aucun éditeur, ni licence de VMS n'est actuellement existant ou fourni sur la préfecture. Il sera donc nécessaire de proposer la fourniture et la mise en service d'un VMS de vidéoprotection à sa dernière version disponible au moment de la mise en œuvre.

Le titulaire devra fournir l'ensemble des licences logicielles nécessaires au bon fonctionnement de la solution proposée.

Ces licences devront couvrir l'intégralité des composants nécessaires à l'exploitation du système, incluant notamment les licences serveur, clients, périphériques, caméras, modules complémentaires ainsi que tout autre élément requis pour un fonctionnement complet et pérenne de l'infrastructure.

La solution de vidéoprotection sera portée par un VMS (**Video Management System**) qui sera à la fois le superviseur de la solution de sûreté. Il sera un programme professionnel référencé comme un grand standard du marché, totalement ouvert, compatible et évolutif aux autres solutions logicielles de la sûreté bâtiminaire. Il ne sera en aucun cas propriétaire et pourra gérer un nombre de périphériques vidéo, d'anti-intrusion et de contrôle d'accès non limité. Le VMS attendu sera de type GENETEC ou équivalent.

L'ensemble de ses licences devront être proposées par le candidat.
À ce titre, le titulaire devra :

- fournir les licences nécessaires à l'intégration des équipements;
- permettre l'exploitation des flux vidéo, l'enregistrement, la consultation, la recherche et la relecture des séquences vidéo depuis les postes opérateurs;
- garantir l'interopérabilité avec les équipements et serveurs déjà en service.

La solution proposée devra permettre une administration centralisée du système, la gestion des droits utilisateurs, la supervision des équipements ainsi que la traçabilité des accès et des actions réalisées par les opérateurs.

L'ensemble des licences fournies devra être perpétuel ou assorti d'un contrat de maintenance et de mise à jour, conformément aux recommandations de l'éditeur, et être livré avec la documentation associée.

7.2.3 LES POSTES DE VISUALISATION, D'EXPLOITATION ET D'EXTRACTION

7.2.3.1 POSTE DE RENVOIE D'IMAGES DE L'HÔTEL DE POLICE

L'Hôtel de Police de Tulle dispose actuellement d'un poste de renvoi vidéosurveillance permettant la visualisation des caméras de la préfecture. Ce poste, est actuellement situé dans la bulle sûreté, devra être remplacé puis migré au sein de la bulle sûreté « DMZ », conformément à la nouvelle solution de vidéosurveillance.

7.2.3.2 LES FONCTIONNALITÉS ATTENDUES

L'exploitation du système de vidéoprotection reposera sur deux catégories de postes, correspondant à des usages et des équipements distincts :

- **Postes de visualisation** : destinés uniquement à l'affichage des flux vidéo en temps réel. Ces postes devront permettre l'affichage simultané de jusqu'à 16 flux vidéo en multi-vues, via un décodeur vidéo associé à un ou plusieurs écrans.
- **Postes d'exploitation** : en complément de l'annexe 6, ce poste est destiné à l'exploitation complète du système, permettant l'affichage des flux vidéo en temps réel, la relecture des enregistrements, ainsi que l'accès aux fonctions d'administration du système. Il permet de plus :
 - L'affichage de la cartographie avec action des caméras.
 - Le pilotage de l'ensemble des caméras et l'affichage des images en cascade ou en mosaïque au choix de l'opérateur, avec possibilité d'afficher en plein écran l'une ou l'autre des caméras par un simple clic de souris. Affichage sur écran dont les caractéristiques techniques sont définies dans l'annexe 6.
 - La gestion du fil de l'eau des événements. Affichage sur écran dont les caractéristiques techniques sont définies dans l'annexe 6.
- **Postes d'extraction** : en plus d'avoir les fonctionnalités du poste d'exploitation et de l'annexe 6, le poste d'extraction d'images permettra aux utilisateurs ayant les droits de gérer l'exportation des séquences vidéos.
 - Les ports USB ne seront pas neutralisés afin de permettre une extraction sur support externe.

7.2.4 LES POSTES À FOURNIR

7.2.4.1 POSTES DE VISUALISATION (qté 3)

- a) 1x Poste de visualisation Vidéo – **Accueil** sans écran (fourniture 1x écran 27" par la préfecture)
- b) 1x Poste de visualisation Vidéo – **Préfet** sans écran (fourniture 1x écran 27" par la préfecture)

- c) 1x Poste de visualisation Vidéo – **Standard** avec fourniture et pose 1 écran 40/42" et support mural

7.2.4.2 POSTE D'EXPLOITATION VIDÉO (qté 3)

à créer par des Unités Centrales et leurs moniteurs :

- a) 1x Poste d'exploitation Vidéo - **COD** sans écran (fourniture 1x écran 27" par la préfecture)
- b) 1x Poste d'exploitation Vidéo – à **l'Hôtel de Police de Tulle** sans écran (fourniture 1x écran 27" par la préfecture)
- c) 1x Poste d'exploitation Vidéo – **Bureau SIDSIC** sans écran (fourniture 1x écran 27" par la préfecture)

7.2.4.3 POSTE D'EXPORTATION VIDÉO

L'un des postes énuméré ci-dessus sera aura la fonction d'extraction.

Écran sur poste d'exploitation vidéo

7.2.4.4 ÉCRAN 40/42 " SUR POSTE DÉJÀ EXISTANT (Qté 1)

- a) Fourniture et pose 1 écran 40/42" et support mural sur le Poste d'exploitation Intrusion – DDS (poste déjà existant). Ce poste sera à équiper de la licence pour l'exploitation de la vidéo (VMS) et (servira également pour l'exploitation et la gestion du contrôle d'accès)

7.2.4.5 CARACTÉRISTIQUES TECHNIQUES DES POSTES

- **Poste de visualisation**

Les décodeurs vidéo 4K avec sortie HDMI devront avoir à minima les caractéristiques suivantes :

- Vidéo 4K avec sortie HDMI
- PoE ou CC
- Sortie audio
- Séquençage fluide et 16 flux dans une vue multiple.

- **Poste d'exploitation / Poste d'extraction**

Les stations de travail devront avoir à minima les caractéristiques suivantes :

- processeur Intel® Core Processor i7- 13700, 4,9Ghz, 5,4 GHz Turbo, 30MB, 8C
- 16GB de RAM
- disque dur de Solid State PCIe NVMe M.2, 256GB (Class 40)
- une carte graphique NVIDIA Quadro
- OS Windows 11 Professional License Desktop, supérieur ou équivalent.

7.2.5 LES CAMERAS

Le titulaire devra procéder à la fourniture et à l'installation de l'ensemble des caméras prévues dans le cadre du présent marché.

Dans le cadre d'une stratégie RSE dans laquelle s'est engagée le ministère, les caméras déployées respecteront les enjeux sociaux et environnementaux prévus par cette démarche. Les caméras seront de constructions européennes afin de privilégier les circuits courts d'approvisionnement. Précisions, particularité : certains sites peuvent demander une **couleur de RAL** spécifique pour une ou plusieurs caméras. Ce besoin peut être évoqué et demandé par exemple lors de la visite de site ou ultérieurement à la visite. **(La préfecture de Tulle est classée monument historique).**

L'ensemble du matériel à installer, y compris les accessoires tels que les boîtes de raccordement, les cols de cygne et autres accessoires sont à fournir. Les caméras sont réparties par modèle selon un plan d'implantation préétabli, qui sera remis au titulaire lors de la visite de site. L'implantation des équipements devra respecter l'implantation sur les plans fournis. Cependant, le soumissionnaire aura tout de même la latitude de proposer un positionnement des dites caméras afin de respecter les zones à surveiller indiquées par l'administration.

La fourniture et l'installation, autant que de besoin soit en nombre suffisant à définir par le soumissionnaire, de caméras numériques IP compatibles ONVIF intérieures et/ou extérieures afin de couvrir l'intérieur et/ou l'extérieur des locaux.

Le titulaire devra noter que, selon la position et le type de caméra, certains accessoires nécessaires à l'installation sont à fournir pour garantir une installation complète et conforme aux prescriptions.

L'installation comprendra, sans s'y limiter :

- le montage mécanique des caméras sur leurs supports ou fixations prévues,
- le raccordement réseau, en conformité avec les prescriptions ministérielles et les normes en vigueur,
- la connexion au VMS et aux postes d'exploitation,
- le réglage et orientation des caméras selon les angles et zones de couverture indiqués sur les plans d'implantation.

Le titulaire devra veiller à minimiser toute gêne ou risque de dommage aux infrastructures existantes lors de l'installation, et à respecter strictement les règles de sécurité applicables aux interventions sur site.

L'ensemble des caméras seront raccordées sur les locaux techniques désignés par l'administration ou proposés par le soumissionnaire.

En cas de coupure de l'éclairage, elles doivent rester opérationnelles et leurs images ne doivent pas être entachées d'une perte de qualité notable.

Leur type est simplement cité comme base de travail. Le soumissionnaire pourra, s'il le juge opportun, proposer un autre modèle à convenir avec l'administration.

Exemple :

- Précision pour la caméra (CamX) :
- Décrire le positionnement, le champ de vision (70°, 180°)

Toutes les caméras seront raccordées à la charge du titulaire en respectant les règles de l'art (cf. §12 page 54.) par un câblage capillaire soit en cuivre, de type « Ethernet/IP », catégorie 6^A / classe E^A , catégorie 7 ou par fibre optique au local technique du bâtiment le plus proche sur un commutateur fourni, configuré et installé par l'administration en collaboration avec le soumissionnaire. Ce dernier fournira la totalité des modules Gbics cuivre ou optique nécessaires au raccordement de la totalité des caméras aux vecteurs de transport mais aussi à la connexion de ces derniers aux commutateurs réseaux de concentration.

Toutes les caméras, de type « Ethernet/IP », seront raccordées au réseau sûreté dont le cœur est installé dans le local technique par un lien cuivre « Ethernet » catégorie 6^A / classe E^A ou de catégorie 7,

Toutes les caméras intérieures et/ou extérieures seront positionnées sur le plan qui sera remis au soumissionnaire lors de la visite de site.

Les caméras, de type « Ethernet/IP » avec les caractéristiques minimales exigées suivantes: ONVIF, WDR, 802.1X, SRTP.

Les caméras sont listées ci-après :

12x Caméras Bullet Extérieur – IR 50m

1x Caméra Bullet Extérieur – IR 80m

2x Dômes Fixe Extérieur – IR 20 ou 30m

1x Caméra panoramique Extérieur 180° - IR, ou faible luminosité

7x Caméra Mini-Dome Interieur – IR 20 ou 30m

Fonction :

- Ambiance = 20 pixels par mètre du champ de visualisation
- Reconnaissance = 120 pixels par mètre du champ de visualisation
- Identification = HD à 24 images/seconde, sous dôme anti-vandale et au format H. 264 (minimum). Elles seront de type jour/nuit. La reconnaissance des personnes sera privilégiée avec une résolution minimale de 600 pixels par mètre linéaire,

8 DESCRIPTIONS DÉTAILLÉES - CONTRÔLE D'ACCÈS

ATTENTION !

Il sera réalisé conformément aux principes décrits dans l'annexe à ce CCTP dénommée :

ANNEXE 2 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE ACCÈS

Le candidat prévoira la fourniture, le raccordement et l'installation :

- autant que de besoin, soit en nombre suffisant à définir par le titulaire des unités de traitement de porte et des unités de traitement local.
- autant que de besoin tel que défini par la maîtrise d'ouvrage, de lecteurs de badges afin de protéger et contrôler les portes indiquées par l'administration.
- autant que de besoin tel que défini par la maîtrise d'ouvrage, d'équipements de verrouillage.

L'ensemble des portes seront majoritairement contrôlées par lecteur de badge en entrée, sortie libre. Certains accès peuvent être contrôlés en entrée et en sortie.

8.1 CONTRÔLE D'ACCÈS EXISTANT ET LE GAC DISPONIBLE

Le contrôle d'accès existant est obsolète. Vous pourrez relever, au besoin, le type et la marque du fabricant lors de la visite sur site.

L'ensemble des lecteurs seront à déposer et remplacer ainsi que l'ensemble des câblages.

Cependant, il est à prendre en considération que la solution portant la solution de détection intrusion est portée par la solution XSECUR'-EVO du fabricant SYNCHRONIC via une UTL et des cartes UTR.

Cette solution est installée en Machine Virtuelle sur le serveur principal DELL R760XS dans l'exercice budgétaire précédent de 2025.

Ce GAC va être une solution centralisée départementale. A l'avenir les sites distants tel que la ou les sous-préfectures, la cité administrative ... seront

également équipées d'un système de contrôle d'accès qui sera raccordé à la base de données du serveur départemental hébergé à la préfecture de Tulle.

Nous sommes en possession du D.O.E. de l'installation existante (intrusion réalisée en SYNCHRONIC en 2025-2026) à jour. Ce DOE pourra être transmis au titulaire.

La base de données du système de contrôle d'accès sera de type SGDBR (Système de Gestion de Base de Données Relationnelle). Les bases de données dites «propriétaires» seront proscrites. Le soumissionnaire indiquera dans son offre son choix de base de données (éditeur, type de licence, etc.)

La solution de contrôle d'accès déployée permet la mise en place de bus terrain sécurisé certifié ANSSI.

La solution devra pouvoir gérer la technologie DESFIRE EV1/EV2 et EV3 compatible carte agent architecturée autour de la puce JCOP 4.5 de la nouvelle carte agent et compatible avec l'ancienne carte (puce OBHERTUR).

Le soumissionnaire indiquera dans son offre le nombre de profils de cartes agents différents que le système choisi permet de gérer.

Le système doit-être évolutif et éprouvé.

A noter:

- Le soumissionnaire fournira obligatoirement un synoptique de fonctionnement détaillé de l'installation qu'il propose. Il développera un descriptif expliquant le fonctionnement de la solution.
- Le soumissionnaire expliquera la méthodologie d'intégration de la solution qu'il propose, avec une description particulière de l'analyse fonctionnelle qu'il mettra en œuvre. accompagnée d'un calendrier prévisionnel de déploiement. La fourniture de ce document est obligatoire et son absence dans l'offre du soumissionnaire est éliminatoire.

8.2 LES ACCÈS CONTRÔLÉS

Il y a déjà des accès contrôlés existants raccordés sur un système obsolète.

Comme stipulé dans l'annexe 2, le contrôle d'accès ne perturbe pas, ne bloque pas, et ne neutralise pas les dispositifs de libéralisation d'ouvrants installés au titre de la sécurité incendie.

Si le cas se présente, le titulaire devra obligatoirement en aviser l'administration qui dépêchera le service ou le coordonnateur en charge du volet « sécurité incendie ».

En cas d'incendie ou d'urgence, les portes des issues de secours seront déverrouillées, sauf avis contraire dans le document descriptif du projet, selon le cas, par :

- déclenchement manuel DMD (Art C046 règlement ERP),
- déverrouillage général déclenché par la Détection Incendie du Bâtiment (raccordement et câblage à prévoir dans la prestation),
- l'UGCIS (Unité de Gestion Centralisée des Issues de Secours),
- clé de secours en cas de coupure de courant.

8.3 LES UNITÉS DE TRAITEMENT LOCAL (UTL)

Sur la préfecture, le nombre d'unités de traitement local, sur laquelle est raccordés les cartes UTR à la préfecture est de 1 de la XSECUR-EVO avec un ou plusieurs BUS câblés.

Le nombre d'unités de traitement local sera déterminé proportionnellement au nombre d'ouvrants à contrôler en respectant les règles de l'art émises par le constructeur.

Elles seront installées dans les locaux techniques désignés par l'administration pour bénéficier entre-autres de l'énergie secourue.

Afin de pouvoir en déterminer leur nombre, le soumissionnaire se reportera aux plans du bâtiment. A défaut, le soumissionnaire proposera une solution alternative qui devra être validée.

Un point d'accès « Ethernet » catégorie 6_A / classe E_A ou supérieur sera créé entre la ou les UTL présente-s dans le local et la baie hébergeant le commutateur « sûreté ».

L'autonomie attendue des alimentations en cas de perte d'énergie, sera de 30 minutes minimum.

L'autonomie estimée de chacun coffret secourue devra être justifiée par la production d'un bilan de puissance par le soumissionnaire dans son offre.

8.4 LES UNITÉS DE TRAITEMENT DE PORTE (UTP)

Le nombre d'unités de traitement de porte sera déterminé proportionnellement au nombre d'ouvrants à contrôler en respectant les règles de l'art émises par le constructeur.

Les modules de portes (UTP) pourront être déportés et installés dans les locaux techniques proches des portes à défendre.

Afin de pouvoir en déterminer leur nombre, le soumissionnaire se reportera aux plans du bâtiment et sur les propositions de rattachement listées ci-dessous. A défaut, le soumissionnaire proposera une solution alternative qui devra être validée.

L'autonomie estimée de chacun coffret secourue devra être justifiée par la production d'un bilan de puissance par le soumissionnaire dans son offre.

8.5 LES LECTEURS DE BADGES (LB)

Les lecteurs de badges existants doivent être $\pm$ au nombre de 30. Ils sont à remplacer.

Il faudra y ajouter la création des 5 nouveaux accès avec lecteurs de badge. Leur équipement de verrouillage et environnement de porte sont également à prévoir tout comme leur ferme porte.

Le présent lot doit, la pose ou le remplacement, le raccordement et l'intégration au système de contrôle d'accès des lecteurs de badges.

Le candidat devra prévoir dans son offre la fourniture des lecteurs en quantité suffisante pour assurer le remplacement des lecteurs existants ainsi que l'équipement des nouvelles portes à créer.

Le candidat devra également fournir les licences nécessaires à l'ensemble de la solution et notamment à l'ensemble des lecteurs de badges.

Le présent lot couvre la fourniture, la pose, le remplacement, le raccordement et l'intégration des lecteurs de badges au système de contrôle d'accès. L'offre devra inclure un nombre suffisant de lecteurs pour assurer :

- le renouvellement des équipements existants,

- l'équipement des nouvelles portes à créer.

Les lecteurs devront répondre aux critères suivants :

- Origine et compatibilité : Fabriqués en Europe, ils devront être compatibles avec les cartes étatiques françaises (AGENT, CIMS, STITCH, IPAF, CPS3 et CPx).
- Normes applicables : Conformité aux normes CE, FCC, UL, RCM, RoHS et REACH.
- Sécurité et fonctionnalités :
 - Support du Proximity Check pour une protection renforcée contre les attaques relais.
 - Compatibilité MIFARE DESFire EV2/EV3 pour une sécurité optimale des données.
 - **Antenne en façade pleine surface**, garantissant une zone de lecture optimisée.
 - Distance de **lecture minimale de 8 cm** avec un badge MIFARE® DESFire® EV2 ou Classic (les lecteurs fins, limités à 6 cm, seront rejetés).

Adaptation aux environnements spécifiques

- **Surfaces métalliques** : En cas de pose sur un support métallique, le titulaire devra prévoir un support d'écartement (Spacer) pour garantir une lecture optimale dans un environnement difficile.
- **Usage extérieur** : Les lecteurs installés en extérieur seront équipés d'un **boîtier antivandale**, conformément aux exigences de sécurité du site.

8.6 ÉQUIPEMENTS DE PORTES

Toutes les portes sous contrôle d'accès existant sont équipées de dispositifs de verrouillages électriques (serrures simples ou motorisées, serrure électromécanique) d'un niveau de sécurité équivalent au niveau de résistance à l'effraction de la porte concernée. Ces dispositifs doivent empêcher toute entrée illicite, y compris en cas de déclenchement du SSI, les sorties pouvant se faire librement dans tous les cas (hors zone de sûreté).

Ces équipements doivent être conservés en l'état.

Les alimentations des portes existantes ne sont pas énumérées dans ce CCTP.

Le présent lot doit le raccordement et l'intégration au système de contrôle d'accès des serrures électriques.

Le titulaire du lot sûreté devra proposer des solutions adaptées afin que huisseries, serrureries et contrôle d'accès assurent la pleine fonctionnalité de la solution globale de sûreté le cas échéant.

La serrurerie sera installée en respectant les règles de l'art et les prescriptions.

Toutes les portes, hors les portes de recoupement, doivent pouvoir être fermées à clé. Une gestion des clés sera assurée par le service utilisateur des locaux.

Toutes les portes sous contrôle d'accès seront équipées de dispositifs de verrouillages électriques (serrures simples ou motorisées, serrure électromécanique) d'un niveau de sécurité équivalent au niveau de résistance à l'effraction de la porte concernée. Ces dispositifs doivent empêcher toute entrée illicite, y compris en cas de déclenchement du SSI, les sorties pouvant se faire librement dans tous les cas (hors zone de sûreté).

Si elles sont requises, seules les serrures électriques présentant les caractéristiques énoncées dans l'annexe 2 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE ACCÈS.

Dans le cadre ce projet, d'une part les équipements de verrouillage existants seront conservés, et d'autre part, les équipements de verrouillage pour les créations des accès seront fournis par le soumissionnaire. Le soumissionnaire devra prendre en compte cette prestation dans son offre du point de vue techniques et financiers.

I'ANNEXE 2 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE ACCÈS

Précision concernant les serrures pour l'accès aux locaux techniques le cas échéant :

Elles seront du type serrures électromécaniques 1 point.

Chaque serrure est commandable individuellement par les lecteurs de badges de ces accès.

Ces serrures seront munies d'une batterie de secours.

La porte sera munie d'une serrure de secours mécanique avec protège cylindre de norme A2P* minimum, dont l'ébauche de clé est protégée.

Nota : Le service conviendra par avance avec la gouvernance collégiale du projet des conditions d'installation des serrures de secours définitives et de remise des clés correspondantes pour les portes du service. Celles-ci, ainsi que la carte propriétaire, devront être remises sous pli scellé opaque au chef de service de la Direction ou son représentant. Les serrures de secours définitives ne devront en aucun cas être installées lors de la phase de travaux et aucune clé ne devra être en circulation.

L'autonomie estimée de chacun coffret secourue devra être justifiée par la production d'un bilan de puissance par le soumissionnaire dans son offre.

8.7 LA DÉTECTION INTRUSION EXISTANTE (HORS LOT)

Le système de détection intrusion à la préfecture est constitué de :

- 16 modules UTR
- +/-9 claviers de mise en / mise hors de cette même génération.

8.8 LES POSTES D'EXPLOITATION ET D'ENCODAGE

Le poste utilisé pour la gestion de l'Intrusion, installé dans le bureau DDS servira également à l'encodage des badges et à la gestion du contrôle d'accès. Il sera, si nécessaire, à pourvoir de la licence logicielle pour faire de l'exploitation et l'encodage du contrôle d'accès.

Ce poste sera à équiper d'un lecteur RFID encodeur/enrôleur de la solution logicielle. Il permettra aux utilisateurs ayant les droits d'enrôler les badges (carte Agent ou blanche). Ils permettent aux utilisateurs ayant les droits, d'administrer le système de contrôle d'accès (administrateur des droits).

Afin de pouvoir utiliser la solution métier de l'administration. 1 lecteur d'encodage complémentaire est à prévoir sur un poste d'exploitation de l'administration raccordé au RIE. Ce poste permet entre autres de créer le conteneur de contrôle d'accès dans le badge agent.

Ces 2 lecteurs d'enrôlements à fournir, seront de marque HID OMNIKEY 5422, STID ou équivalent en version USB.

Un poste prévu dans le bureau SIDSIC, prévu dans le chapitre vidéo, sera également à pourvoir d'un lecteur encodeur USB et de la licence de gestion de contrôle d'accès. Et 2ème lecteur pour la solution métier de l'administration.

8.9 LES BADGES

Type de badge (CAM)

LA SOLUTION DE CONTRÔLE D'ACCÈS DOIT ÊTRE COMPATIBLE AVEC LA CARTE AGENT DU MINISTÈRE DE L'INTÉRIEUR

La solution doit permettre la gestion de différents types de badge portés par des modèles de badge différents. On différenciera naturellement le type de badge, des droits ou profils liés à chaque badge.

Pour simplifier les choses et pour ne pas dévoiler d'informations vitales, il existe au niveau de la personnalisation des badges à minima les catégories suivantes pour les personnes :

- Badge **P** : badge nominatif pour les **permanents** toutes directions confondues ; La personnalisation graphique varie pour les badges de la classe P,
- Badge **V** : badge non nominatif, journalier, pour des **visiteurs** occasionnels externes. Les droits d'accès associés aux badges V sont définis par le bureau des badges. Ce sont des droits minimums.

La carte sans contact, de format ISO 7816 avec capacité sans contact ISO 14443, utilisée pour l'identification aux contrôles d'accès est fondée sur la puce Mifare DesFire EV1/EV2/EV3.

Le titulaire devra la livraison de 100 badges, PVC blanc, format ISO 7816 avec capacité sans contact ISO 14443, badge vierge, libre de droit, tel que sorti d'usine, sans modification de clés (clé maître notamment) ni de droits.

9 DESCRIPTIONS DÉTAILLÉES - VISIOPHONIE

9.1 DESCRIPTION DE L'EXISTANT

Les interphones et visiophones en place sont obsolètes et certains ne fonctionnent plus.

9.2 DESCRIPTION DÉTAILLÉE DES PRESTATIONS À RÉALISER

Le soumissionnaire fournira les interphones et les postes de réception.

L'intégration des visiophones dans la solution vidéo est demandée (interfaçage visiophonie/solution vidéo).

Le soumissionnaire prévoira également la refonte du câblage (Dépose, dépollution et tirage de nouveaux câbles)

V : Visiophone

PR : Poste de Réception

Fourniture, installation, mise en service et programmation

Ouvrant	Réf.	Quantités et type			Exemple Direction visio.
		VE	VI	PR	
Écran 7 '' ou équivalent – Accueil				1	
Écran 7 '' ou équivalent – Résidence du préfet				1	
Écran 7 '' ou équivalent – Standard				1	
1x Visiophone 2BP – Entrée Principale public		1			Accueil & Standard
1x Visiophone 2BP – Portail d'honneur		1			Résidence Préfet & Standard
1x Visiophone 2BP – Portail Parking et Barrière		1			Standard
Total visiophone extérieur		3			
Total visiophone intérieur			0		
Total poste de réception				3	

- Prévoir, réaliser, et paramétrer en fonction d'une analyse fonctionnelle, l'asservissement entre les systèmes de contrôle d'accès et la visiophonie. C'est-à-dire que de part un poste de réception visiophones, il devra être possible d'ouvrir une porte. Le système de visiophonie devra donc communiquer avec le système de contrôle d'accès pour autoriser proprement l'action.

Intégration à la solution vidéo

Le soumissionnaire proposera l'interfaçage du système de visiophonie avec sa solution de supervision vidéo (VMS).

Les images de visiophones devront pouvoir s'intégrer dans le système d'affichage comme toute autre caméra du dispositif ou être présentées en incrustation sur le même écran.

L'interfaçage avec le système de vidéo sera également demandé afin de pouvoir enregistrer les images et gérer, selon les cas, les accès à partir des postes d'exploitation sans utilisation de pupitre dédié.

Le son issu des platines de visiophones transitera par la carte audio du PC d'exploitation vidéo.

La restitution du son sur les écrans d'affichage des images sera privilégiée par rapport à des enceintes externes.

En aucun cas, le son ne sera enregistré.

LES LICENCES VMS

Le soumissionnaire devra proposer la fourniture des licences et la mise en service des visiophones sur le VMS de vidéoprotection à sa dernière version disponible au moment de la mise en œuvre.

Le titulaire devra fournir l'ensemble des licences logicielles nécessaires au bon fonctionnement de la solution proposée.

9.3 DESCRIPTION TECHNIQUE

Dans le cas d'une nouvelle installation, il sera déployé de préférence un système de technologie IP qui aura les caractéristiques suivantes :

Platine Vidéo:

- Platine anti-vandale, de préférence encastrée si la configuration du site le permet
- Impérativement muni de LED IR,
- Objectif grand-angle et zoom
- Technologie IP SIP (Session Initiation Protocol)
- Si demandé lors de l'analyse fonctionnelle, ce portier pourra être associé à une caméra IP.

De plus, la platine vidéo de rue, installée à l'entrée du public, sera conforme à la norme accessibilité des ERP (Loi 2014-789 du 10 juillet 2014).

- Boucle magnétique conforme à la norme NF EN 60118-4:2007
- Pictogrammes (appel en cours, parler, ouverture porte)
- Synthèse vocale (appel en cours, parler, ouverture porte)

Moniteur Vidéo :

- Ecran LED de 7 pouces minimum,
- Support mural ou de bureau,
- Commandes de portes par touches dédiées ou écran tactile

Le système peut comporter plusieurs platines ou plusieurs moniteurs. L'ensemble sera programmable à l'aide d'une interface Web.

Décrit en annexe 6 ANNEXE 6 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES VIDÉO PROTECTION 2024 § 7.

10 INTERFONCTIONNEMENT DES SYSTÈMES

D'une façon générale, le volume (nombre de périphériques) des solutions de sûreté déployées par le ministère ne justifie pas l'intégration d'un hyperviseur. Le rôle de l'hypervision sera assuré par les briques natives de supervision présentes dans le VMS ou G.A.C de la solution de sûreté.

La supervision de la solution sera réalisée par une interface unifiée assurant la gestion de la vidéosurveillance, du contrôle d'accès et de l'anti intrusion.

A l'avenir, la supervision sera donc réalisée à partir du VMS.

Tous les événements (identifiant, alarmes, sorties, entrées, états) liés à un point d'accès ou un point d'intrusion sont horodatés et enregistrés. Ces événements indexent les flux vidéo des caméras associés au point d'accès ou d'intrusion.

Tous les événements associés aux points d'accès supervisés par le système vidéo sont liés aux images correspondantes et accessibles par simple clic dans l'interface de supervision.

A l'avenir, les alarmes seront couplées au système vidéo pour l'enregistrement, la levée de doute avec pré-positionnement sur les zones en alarme et naturellement l'interface de traitement et d'acquittement.

Les alarmes seront affichées avec toutes les possibilités vidéo associées de la visualisation des points de fuite.

Le serveur de temps (NTP) sera la référence d'horodatage de l'ensemble de la solution, fourni par l'administration.

11 LA CYBERSÉCURITÉ

Cybersécurité (obligatoire selon ANSSI et CCN) :

Le titulaire devra intégrer les machines virtuelles sur les serveurs existants, principal et de redondance, et en PSE assurer le paramétrage des certificats RADIUS nécessaires au fonctionnement du service.

Pour information la VM Radius devra correspondre à l'architecture de protection en cybersécurité sera constituée de 4 briques :

Brique de sécurité N°1 :

Les flux vidéo entre les caméras et les serveurs seront chiffrés par activation du protocole SRTP (Secure Real Time Protocol) conformément à la recommandation RFC 3711.

Les équipements déployés dans la solution devront être compatibles avec ce protocole.

Brique de sécurité N°2 :

Les flux d'administration entre les serveurs et les autres équipements raccordés sur le réseau de sûreté bâtementaire (serveurs et périphériques tels que caméras..) seront chiffrés par activation du protocole HTTPS (HyperText Transfer Protocol Secure) conformément à la recommandation RFC 2818. HTTPS sera déployé sans certificat auto-signés. Les certificats auto-signés, sans autorité tierce, sont proscrits.

Brique de sécurité N°3 :

Contrôle d'Accès : Chaîne de sécurité sans faille du badge jusqu'au serveur de gestion de la solution de CA. L'ensemble des matériels (UTL, modules d'extension, lecteurs,..) et logiciels proposés devront être conformes aux recommandations du guide de l'ANSSI : « SECURITE DES TECHNOLOGIES SANS CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES » (Version du 19/11/2012) selon l'architecture 1 de façon native sans convertisseur. La solution devra être sécurisée de bout en bout, du badge jusqu'au serveur. Les principes et fonctionnalités suivants devront être disponibles et réalisés par les équipements et logiciels fournis : Conforme ANSSI architecture 1, La solution devra être compatible avec le réseau VLAN, VPN du site, La solution devra être compatible avec l'annuaire LDAP du site pour la

gestion des opérateurs et de leurs droits, Communications réseau IP cryptées TLS AES 256 bits et signées (intégrité et authentification) entre le serveur et les UTL d'une part et les postes clients d'autre part, Communications bus RS485 cryptées AES 128 bits et signées. Toutes les clés de communications sur IP et RS485 devront être changées périodiquement de manière automatique par le système sans action humaine pour durcir le cryptage contre toute malveillance, Le client final aura obligatoirement la maîtrise de sa clé de communication initiale, qui créera automatiquement les clés suivantes périodiquement, par la saisie, sur un poste client lourd, de cette clé (cérémonie des clés), Protection des attaques par déni de service (DoS) par le Firewall des automates UTL. Paramétrage de la configuration IP des UTL à travers un Web serveur embarqué sécurisé HTTPS, SSH, UTL compatible avec serveur radius 802.1X. Le module de porte communiquera en bus RS485 crypté AES128 bits avec les lecteurs e protocole SSCP V2 sera activé pour le chiffrement des flux de données entre les lecteurs de badge contrôlant les portes, et les unités de traitement de porte de la solution de contrôle d'accès.

Brique de sécurité N°4 :

Un serveur d'authentification RADIUS, local ou zonal selon les directives de l'administration, sera pré-installé par activation du protocole 802.1 X (avec certification EAP-TLS) sur le réseau de sûreté bâtementaire afin garantir la sécurité des ports des commutateurs réseaux et autres équipements raccordés sur ce réseau. Les ports non utilisés des commutateurs réseaux et autres équipements raccordés seront neutralisés logiquement par programmation et physiquement par des bouchons, même dans les baies de sûreté bâtementaire. Cette préparation permettra d'intégrer le service Radius sans avoir à reconfigurer l'ensemble du système lors de l'accueil de la vidéosurveillance.

Le serveur d'authentification Radius sera implémenté en machine virtuelle sur le serveur physique principal de la solution de sûreté, et en cas de présence d'un serveur physique de secours, il sera aussi implémenté en machine virtuelle sur ce serveur redondant.

Il ne sera en aucun cas installé sur un serveur physique indépendant et isolé sur le réseau.

Le protocole FTP (File Transfert Protocol) sera désactivé et les guides de durcissement des constructeurs des équipements déployés seront appliqués.

Les certificats auto-signés, sans autorité tierce, sont proscrits. Ils seront générés par un service d'authentification tierce géré par un Active Directory propose à la solution de sûreté.

Cet AD sera à déployer, dans la VM du Radius, par le soumissionnaire lors de ce renouvellement de la solution de vidéosurveillance.

Les briques de cybersécurité devront être installées sur les serveurs.

Le réseau déployé sera conforme au Cahier des Clauses Techniques Simplifiés de Cybersécurité pour les marchés publics (arrêté du 18/09/2018), au Règlement Général de Sécurité de l'ANSSI.

12 COURANT FAIBLE, COURANT FORT, ÉTIQUETAGE

12.1 POINT PARTICULIERS A NOTER

L'ensemble des câblages IP et 230V nécessaires à l'alimentation des postes informatiques, tels que décrits dans le présent CCTP pour la Préfecture de Tulle, sont déjà en place. Le Cas échéant, de nouvelles liaisons devront être tirées et installées pour assurer le raccordement des postes d'exploitation, de visualisation et d'extraction.

12.2 COURANT FAIBLE

Pour information :

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, caméras, UTL, etc.) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (et dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 6A / classe EA ou catégorie 7 en respectant les règles de l'art.

Les commutateurs et le serveurs sont installés dans les baies de sûreté, suffisamment dimensionnées afin d'accueillir la totalité des équipements de la solution.

La fourniture des accessoires nécessaires pour le câblage de ces baies est à prévoir et sera à la charge du soumissionnaire.

Tous les câblages, fibre optique ou Ethernet, en extérieur (façade) comme en intérieur dans les passages accessibles au public, **seront protégés par des goulottes métalliques type oméga.**

12.3 CAPILLAIRE CUIVRE

Le capillaire cuivre fait partie des prestations répondant aux prescriptions de l'annexe du présent CCTP dénommée :

ANNEXE 1 – CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, caméras, etc.) proposés dans la solution seront raccordés sur le répartiteur désigné par l'administration (dans la plupart des cas, le plus proche) par un lien « Ethernet » catégorie 6A / classe EA ou catégorie 7 respectant les règles de l'art.

L'établissement de ces liens fait partie des prestations répondant aux prescriptions de l'annexe.

12.4 COURANT FORT ET ONDULEURS

Tous les organes de sûreté sont raccordés sur le réseau ondulé et ou sur le groupe électrogène.

Alimentation en énergie électrique ondulée et secourue

Le soumissionnaire prévoira d'installer pour la baie du serveur redondant l'onduleur déjà fourni suite à exercice budgétaire précédent et est toujours sous carton.

Les onduleurs secourent les serveurs et les commutateurs sûreté dans le cadre de ce projet.

Ils sont pourvus de carte SNMP permettant de communiquer en IP avec le serveur et d'assurer sa coupure proprement dès que sa charge tombe sous les 20 %.

Les onduleurs sont répartis de la manière suivante :

Bâtiment	Étage	Répartiteur	Fonction	Onduleur	Carte SNMP
Préfecture	-	-	Répartiteur du serveur Alimentation serveur principal et commutateurs	1	1
Préfecture	-	-	Sous-répartiteur Alimentation serveur redondant et commutateurs	1	1
Onduleurs à fournir, quantité totale :				0	0

Caractéristiques du ou des onduleurs :

- format 19 pouces rackable
- raccordé à l'installation par un circuit 230 V-16 A 2P+T protégé par un disjoncteur différentiel 30mA hautement immunisé (type HI)
- branchement effectué sur la distribution électrique secourue désignée par l'administration
- bandeau électrique 6 prises 2P+T, au format 19 pouces, à fournir, intégrer dans la baie et raccorder sur sa sortie.
- l'onduleur devra maintenir l'alimentation électrique pour une durée minimale de 30 mn.

- autonomie de secours à prévoir de 30 minutes pour chacun des onduleurs.
- une carte SNMP afin de communiquer en IP avec le serveur et d'assurer sa coupure proprement dès que sa charge tombe sous les 20 %.

12.5 ÉTIQUETAGE

Tous les matériels installés au titre du présent marché devront être identifiables au moyen d'une étiquette accessible et visible.

12.6 ACTEUR

Toutes ces prestations sont à la charge du titulaire.

13 LA MAQUETTE

La maquette devra être réalisée exclusivement sur le site de la préfecture, les serveurs, y compris celui hors production, y étant déjà installés.

14 EXPLOITATION DE LA SOLUTION

14.1 GESTION DU SYSTÈME

PRÉSENTATION DES PROFILS UTILISATEURS

L'administration précise les profils utilisateurs en vigueur dans le cadre de la gestion des dispositifs plus généralement de sûreté :

- L'accès « **Administrateur système** » permet à un opérateur clairement désigné et habilité, de vérifier le bon état de fonctionnement du dispositif et d'en administrer l'ensemble (paramétrage, configuration, supervision, sauvegardes, lectures, cartographie...) ainsi que la visibilité des informations qu'il contient,
- L'accès « **Gestionnaire de badges** » permet à un opérateur, sous-réserve de ses droits, d'administrer et gérer les profils, de produire des badges, etc. En aucun cas le profil « Gestionnaire de badges » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système,
- L'accès « **Opérateur** » permet à un exploitant, sous-réserve de ses droits, de consulter la cartographie, gérer des alarmes, produire des badges, gérer des portes, ainsi que de consulter les fiches réflexes, etc. En aucun cas le profil « Opérateur » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.
- L'accès « **Opérateur d'extraction** » permet à un exploitant, sous-réserve de ses droits, de consulter les images, faire des recherches de séquences, extraire des images, etc. (pour le format) En aucun cas le profil « Opérateur d'extraction » ne pourra porter atteinte à l'intégrité des données vidéo enregistrées par le système.

L'implantation des différents terminaux se fera en fonction du choix retenu par le maître d'ouvrage.

14.2 EXPLOITATION PAR L'ADMINISTRATEUR DU SYSTÈME

Le système doit permettre de définir des profils utilisateurs permettant de gérer des « droits » ou privilèges sur les objets Équipement/Événement/Alarmes/Actions/Espace de Travail dans tous les applicatifs utilisés. Cette gestion doit, par exemple, quand l'objet est une action, permettre de définir des droits de Création/ Suppression / Exécution/ Modification.

Toutes les actions sur le système sont réservées et protégées par des droits liés au compte applicatif de l'opérateur. Il y a à minima trois types de droits :

- Le droit de lecture confère à un opérateur le pouvoir de visibilité,
- Le droit d'écriture confère à un opérateur un pouvoir d'action,
- Le droit de modification confère à un opérateur les droits de modification.

14.2.1 CONFIGURATION DES DROITS OPÉRATEURS

Les éléments suivants sont configurés en droits (profil par opérateur), pour permettre à minima les fonctions suivantes :

- Des droits sont gérés pour la création/visualisation/configuration des entités du système (utilisateur, badge, alarme, actions, fiche de porteur, rapport, équipement),
- Des droits sont gérés par équipement pour permettre la création, la visualisation, la configuration, le changement d'état (actif/inhibé),
 - Un équipement (porte, lecteur de badge, détecteur) peut être invisible à un utilisateur,
 - Un équipement (porte, lecteur de badge, détecteur) peut être en accès lecture seule,
 - Une porte en lecture seule doit permettre la visualisation de son état mais inhibe les droits d'actions Ouverture/Fermeture.
- Des droits sont gérés pour les éléments partagés,
 - Infériorisation des commandes joystick,
 - Priorisation sur l'accès à des écrans et vignettes des murs d'images,

- Accès en lecture seule sur la définition des écrans et vignettes des murs d'image,
- Accès en modification seule sur la définition des écrans et vignettes des murs d'image,
- Des droits sont gérés pour la création, la visualisation, le déclenchement des actions programmées ou natives,
- Des droits sont gérés pour la création, la visualisation, la modification de l'espace de travail,
- Des droits sont gérés pour l'accès aux applications de la solution.

Un opérateur « poste de contrôle et de sécurité » doit pouvoir :

- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,
- Disposer de droit en écriture sur un accès pour l'ouvrir/le fermer,
- Visualiser certaines caméras.

Un opérateur « gestionnaire des badges » doit pouvoir :

- Configurer son espace de travail ;
- Créer/modifier des profils, des groupes de porteurs, des porteurs de badge,
- Disposer d'un droit en écriture sur des accès pour l'ouvrir / le fermer,
- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,
- Disposer des droits de lecture/écriture/modification des équipements d'accès,
- Éditer un badge.

Un opérateur « extraction d'images » doit pouvoir :

- Configurer son espace de travail ;
- Recherche des séquences d'images enregistrées sur le stockeur,
- Faire des extractions d'images (lecture seule)

- Disposer d'un droit en écriture sur les ports USB de son espace de travail,
- Disposer d'un retour type fil de l'eau événement/alarme sur les équipements dont il aura la visibilité,

Seuls les opérateurs déclarés avec un profil « administrateur » disposent d'un accès en écriture sur tous les équipements.

Le système de gestion des droits est paramétrable. Le système doit permettre une gestion sécurisée des mots de passe des utilisateurs.

Le système de gestion des droits doit permettre de définir des droits relatifs à la définition/modification de l'espace de travail.

Le système doit avoir une gestion des droits permettant de gérer des équipements partagés ou des informations partageables, que ce soit dans le cadre de « raccordements » (fédération, déport, supervision multi-site) ou dans le cadre d'utilisation locale (partage de la motorisation des caméras, des murs d'images).

La documentation doit fournir une description détaillée des possibilités natives offertes par le système de gestion des droits.

14.2.2 GESTION DES JOURNAUX

La solution doit permettre la consultation de l'ensemble des actions effectuées sur le système que ce soit au niveau des postes clients ou au niveau des postes serveurs mais selon les droits octroyés à l'utilisateur.

Les actions tracées sont à minima :

- Système
 - Arrêt / Lancement des services applicatifs (journalisation incluse),
 - Arrêt critique sur incident,
 - Arrêt système par exploitant (identifiant, date/heure),
 - Démarrage système par exploitant (identifiant, date/heure), Évènement de ressources systèmes;
- Administration applicative
 - Ajout/suppression d'équipements,
 - Gestion des comptes (création/suppression/modification des droits).

- Exploitation courante
 - Heure de connexion, déconnexion,
 - Action sur un équipement,
 - Action sur un badge.

La solution doit protéger cette traçabilité par son système de droits (profil).

14.3 EXPLOITATION PAR LES OPÉRATEURS

GESTION TYPE

14.3.1.1 AMÉNAGEMENT DU POSTE DE GESTION

Ces postes ont été mentionnés dans le chapitre 7.2.3 LES page 33

Ces postes disposeront d'un écran:

- l'écran affichera le plan graphique renseigné du site, en 2D avec noms des lieux, numéro de l'étage, nom ou numéro de la pièce, type et qualité des moyens, ainsi que la disposition des moyens mis en place tels que caméra, détecteur/contrôleur d'ouverture de porte, détecteur de mouvement, le lancement de commandes directes (mise en/hors service de point d'entrée, activation de sortie, déverrouillage d'accès, etc.).

Sur le même écran, **une fenêtre** présentera une fiche « main courante » précisant les événements du jour (prévus, arrivés, en cours, etc.), les incidents types, la conduite à tenir, les mesures prises qui permettent de prévoir, organiser et gérer la sécurité au quotidien en cas d'événement, qu'il soit anodin ou grave. Il sera aussi celui qui permettra l'acquittement et la visualisation des alarmes, la gestion manuelle et automatique des caméras, le pilotage de l'éclairage, l'utilisation des prépositions des caméras sur le plan graphique, l'enregistrement numérique sur disque dur des événements du site).

14.3.1.2 GESTION DES ENQUÊTES

La solution doit permettre la recherche d'événements-alarmes, mémo, signet, métadonnées et de visualiser la vidéo éventuellement associée à l'événement.

14.3.1.3 GESTION DE LA CARTOGRAPHIE

Le système dispose d'un outil de cartographie dynamique permettant de localiser tous les équipements de sécurité (caméra, portillon, porte surveillée, contrôle d'accès, lecteur RFID, haut parleur, sirène, détecteur de présence, etc..) sur un plan. Le plan et ces équipements peuvent s'afficher à l'échelle (proportion respectées), par zone, par bâtiment et par étage.

La cartographie accepte les fonctions de zooms avant/arrière à partir de la molette de la souris (par exemple).

Le système doit permettre de zoomer dans le plan, de se diriger à 360.

Le système dispose d'une cartographie multi sites et multi niveau.

La cartographie doit permettre d'exécuter des actions de type glisser/déposer de la cartographie vers toute vignette d'affichage pour permettre :

- De visualiser une caméra par action de déposer d'une caméra vers une vignette d'affichage,
- De visualiser les événements liés à une porte par action de déposer d'une porte vers une fenêtre,
- De visualiser les photos des titulaires identifiés sur une porte par action de glisser déposer d'une porte vers une vignette d'affichage.

La cartographie doit permettre de proposer une aide contextuelle par équipement. Il devra apparaître un encadré dans lequel devra figurer leur appellation, leur position (étage, zone de sûreté...) et le moyen de détection (détecteur, détecteur/contrôleur, caméra fixe, mobile etc.).

Ce plan graphique, disponible sur les postes d'exploitation, servira en particulier à la visualisation des événements.

Par ailleurs, ces événements entraîneront une animation des éléments graphiques représentant les équipements (barrières infrarouges, détecteurs d'intrusion, caméras etc.) de la zone concernée.

Lorsqu'un événement se produit dans une zone qui est constituée d'une (ou plusieurs) caméra(s) et/ou d'une barrière infrarouge ou autre détecteur de mouvement, chaque équipement de la zone de détection, qui aura déclenché l'alarme, sera automatiquement signalé par un changement de couleur et d'un clignotement sur la cartographie.

Exemple: la caméra de visualisation passe en rouge de même que le (ou les) faisceau(x) franchi(s) reliant deux barrières infrarouges, etc.).

Par contre, ce changement de couleur sera différent suivant l'état du système :

- En rouge lors du déclenchement d'une alarme, restera en rouge tant que l'alarme ne sera pas acquittée,
- En orange lors du déclenchement d'une panne.

14.3.1.4 GESTION DES ALARMES

La solution doit permettre la définition d'une alarme ou d'un événement/alarme à partir de la combinaison d'événements détectés par le système, contact sec, détection d'ouverture, détection d'événements d'identification, d'événements natifs et programmables.

La solution doit permettre de paramétrer la notion d'alarme et d'événement pour pouvoir, sous réserve de ses possibilités, définir une alarme et un événement et éventuellement convertir une alarme en événement (et réciproquement).

Le système doit permettre une hiérarchisation des alarmes par niveau et une hiérarchisation des événements. La solution doit permettre la gestion de 10 niveaux d'alarmes et d'événements. Les niveaux d'alarmes doivent pouvoir être filtrés sur la console opérateur et affichés par des signes distinctifs (couleur, etc..).

Le terme alarme prioritaire utilisé dans ce document est une alarme de niveau 1.

Chaque alarme doit pouvoir être déclarée dans un champ de 1 à 255 caractères.

Le système doit permettre d'afficher une procédure à suivre en « alarme ».

Le système doit permettre de gérer des alarmes notifiées par l'opérateur.

Le système doit permettre une gestion des alarmes en cascades.

14.3.1.5 GESTION DU SYSTÈME VIDÉO ET SCENARIOS

Le ministère souhaite la mise à disposition d'une interface simple pour créer des scénarii d'actions. Ces scénarios sont déclenchés soit par un ou une association d'événements (alarme/calendaire), soit manuellement par l'opérateur.

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements,
- Définir des actions sur des caméras.

Le système de vidéo-détection fera l'objet d'un fonctionnement particulier intégrant les informations ci-après :

- D'une prise en compte de plages horaires,
- D'un déclenchement d'alarme selon la zone de détection,
- D'une localisation sur un plan graphique.

Le système d'acquisition et de visualisation numérique des images doit pouvoir s'activer automatiquement dès le déclenchement de la caméra couplée à la détection de la zone traversée ou de mouvement particulier ou d'objet identifié ou d'interprétation et d'analyse d'images.

Il faut pouvoir créer et gérer pour chaque caméra des scénarii préprogrammés (rondes dans le temps ou rotation dynamique cyclique et cycles d'images pour différents groupes de caméras).

Les caméras peuvent être individuellement programmées sur un scénario qui s'appliquera par défaut, au bout d'un laps de temps sans action (rondes, repositionnements).

- Portes et Points d'Accès :

Les actions natives pour les équipements portes/points d'accès sont : Ouvrir, Fermer, Inhiber.

- Visiophonie :

Les actions natives pour les équipements de visiophonie sont : Ouvrir, Fermer, Inhiber, mettre en attente une communication.

- Point Alarme :

Les actions natives pour les équipements d'alarmes sont : Armer, Désarmer.

- Mur image :

Positionner le mur d'image dans une configuration spécifiée,

L'utilisateur peut pour un scénario nommé :

- Définir des actions sur des portes, passages, équipements de détection d'intrusion,

- Définir des actions sur des caméras.

Exemples de scénarii modifiables :

Scénario 1 : Exploitation « normale de jour »,

Scénario 2 : Exploitation « normale de nuit »,

Scénario 3 : Exploitation « normale de week-end et de jours fériés »,

Scénario 4 : Exploitation en situation normale exceptionnel prévisible (exemple élections, visites de personnalités etc.),

Scénario 5 : Situation de crise.

Pour chaque scénario il sera possible de programmer les fonctions de chaque caméra, les enregistrements à effectuer, les consignes à appliquer en cas d'alarme, etc.

Le passage d'un scénario à l'autre pourra indifféremment se faire automatiquement selon un programme horaire ou une action manuelle par un opérateur autorisé.

14.3.2 PRINCIPE DE GESTION DES RÉACTIONS A ÉVÉNEMENT

Les actions natives sont :

- Acquitter une alarme,
- Afficher un objet du système (fiche carte, fiche utilisateur/voiture, photo d'un identifiant),
- Afficher le signal d'une caméra / les signaux d'un groupe paramétrable de caméras sur une vignette du mur d'image,
- Ajouter un signet et/ou une métadonnée jointe au système vidéo,
- Automatiser la production d'un rapport,
- Déclencher l'asservissement du lecteur vidéo pour rejouer une séquence,
- Déclencher un scénario identifié par un nom,
- Déclencher une ronde vidéo,
- Déclencher/Arrêter un enregistrement,
- Diffuser un message audio depuis un fichier ou un micro,
- Ouvrir ou fermer la sortie relais d'un contrôleur.

Le système doit permettre d'adresser des actions natives et de définir par configuration avec un outil et/ou par programmation des actions « dédiées ».

Le système doit permettre d'associer une action à partir d'une liste d'actions.

Le système doit permettre de déclencher une action calendaire.

Le système doit permettre de déclencher une action programmée c'est-à-dire que toutes les actions sont activables sous la forme de trigger.

Le système doit permettre de gérer manuellement et automatiquement (via les actions) le mur d'image. Il doit par exemple pouvoir afficher une caméra en alarme sur une vignette numérique d'un moniteur informatique local ou distant.

Le système doit permettre de déclencher une action à distance sur un autre sous système dans le cas de raccordement ou d'utilisation multi-sites.

La solution doit permettre à un utilisateur, par une action simple et sous réserve de ses droits, de n'importe quel poste client de :

- Activer / Désactiver un équipement,
- Consulter l'état d'un équipement,
- Créer/Supprimer un équipement,
- Inhiber les alarmes associées à un équipement,
- Ouvrir/Fermer un accès.

Ces actions peuvent être faites directement au niveau cartographique et simplement par l'intermédiaire de menu.

15 EXIGENCES SÉCURITAIRES

Les mesures de sécurité complémentaires suivantes sont à prendre en compte.

N°	Domaine	Description de la mesure	Bien(s) support(s) concerné (s)
1	Organisation de la sécurité des SI	Contrat de maintenance 5j/7 – HO avec intervention sous 24H	UTL, serveurs, lecteurs
2	Organisation de la sécurité des SI	Ajouter à l'ensemble des marchés publics les clauses de sécurité établies par la DSIC (cf site SSI DSIC)	Serveur, UTL, postes administrateur
3	Organisation de la sécurité des SI	Exiger une enquête de sécurité sur les prestataires. Conformément aux PES, les administrateurs encadrent les prestataires pour chaque intervention technique. Pour les travaux nécessitant un accès aux locaux techniques, la présence d'un administrateur MI est obligatoire	Serveur, UTL, postes administrateur
4	Organisation de la sécurité des SI	Interdire la télémaintenance depuis les locaux d'une entreprise privée. La maintenance du SI devra se faire in situ.	Serveur, commutateur, UTL, lecteurs
5	Évaluation de la sensibilité et protection des documents	Protection des clefs de lecture Idéalement : La clé de lecture est répartie sur plusieurs porteurs ; sécurité liée à la gestion (introduction dans la solution) sécurité et inviolabilité des équipements de stockage des clés (lecteurs, coffres pour les badges de configuration éventuels, base de données éventuelles, etc..) sécurité liée au renouvellement ;	Lan Commutateurs, Serveur , UTL, Poste admin , Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
6	Évaluation de la sensibilité et protection des documents	Les clefs et en particulier la clef de lecture, ne doivent en aucun cas être communiquées aux installateurs	Lan Commutateurs, Serveur, UTL, Poste admin , Badges admin, lecteurs, Équipes admin, Badges utilisateurs,
7	Ressources humaines	Formation et sensibilisation des administrateurs SIC aux PES et mesures de sécurité « Contrôles d'accès » et des gestionnaires d'accès aux règles de gestion des accès.	
8	Sécurité physique des locaux	Les équipements seront installés dans des locaux sécurisés par contrôle d'accès	UTL, Poste admin, Badges admin
9	Sécurité physique des locaux	Alimentation électrique secourue – onduleur, groupe électrogène – Climatisation – Détection incendie. En cas de coupure électrique, les portes ou portiques	Lan Commutateurs, Serveur, UTL,

		devront rester, par défaut, en position fermée.	Poste admin , lecteurs,
10	Sécurité physique des locaux	Sécuriser l'accès aux locaux sensibles (locaux techniques,...), par la mise en œuvre d'un second mécanisme de contrôle (ex : digicode ou biométrie). Avec deux mesures à mettre en œuvre : - une mesure technique pour la gestion des droits administrateur applicatifs - une mesure pour le processus de validation des droits	Serveur, commutateurs
11	Architecture et exploitation des SI	Redondance des UTL et répartition des lecteurs d'une même zone sur plusieurs contrôleurs.	UTL, lecteurs
12	Architecture et exploitation des SI	Redondance lecteurs : Utilisation d'un autre accès en cas d'indisponibilité d'un lecteur	Lecteur
13	Architecture et exploitation des SI	Redondance des commutateurs, architecture sécurisée Une architecture 2 minimum serait souhaitable pour disposer des moyens de sécurisation nécessaires. L'objectif est d'assurer un niveau de disponibilité maximum sur les commutateurs avec une durée d'indisponibilité maximum de 24 heures.	Commutateur LAN
14	Architecture et exploitation des SI	Prévoir plusieurs badges administrateurs	Poste admin , Badges admin,
15	Architecture et exploitation des SI Gestion de la continuité des SI	- Sauvegarde quotidienne au minimum des données sensibles (clefs de lecture, profil, logs)	Équipe d'administration Serveur
16	Architecture et exploitation des SI	Mettre en place et vérifier le bon fonctionnement des mises à jour automatiques de l'antivirus de façon régulière sur l'ensemble des équipements informatiques. Appliquer la politique de configuration ministérielle Procéder à une analyse antivirus quotidienne des serveurs	Serveurs, postes admin
17	Architecture et exploitation des SI	Mettre en place les correctifs de sécurité et upgrade applicatifs matériels	Serveurs, postes admin, UTL, Commutateurs, Lecteurs
18	Architecture et exploitation des SI	Autonomie des UTL par rapport aux serveurs : Les UTL doivent avoir une copie de la base des droits afin de continuer à fonctionner de manière autonome. Toutes les UTL pourront fonctionner sans perturbation en cas de perte de la liaison avec les équipements en amont.	UTL
19	Architecture et exploitation des SI	Mettre en œuvre un réseau physique dédié aux équipements contribuant à la mise en œuvre des systèmes de sécurisation. A défaut, une solution basée sur les technologies VPN IPSEC (dont la configuration devra être conforme aux recommandations de l'ANSSI) sera mise en œuvre. L'objectif étant d'isoler les enclaves du système de contrôle d'accès (sous forme de DMZ) et les interconnecter entre	Lan Commutateurs, serveur, UTL, postes administrateur

		elles par VPN IPSEC. Aucune interconnexion ne devra être possible entre le RGT et les enclaves « Contrôle d'accès » entre les VLANs RGT (serveur, postes de travail, ...) d'un site et les enclaves « Contrôle d'accès »	
20	Architecture et exploitation des SI	La communication entre le badge, la tête de lecture et l'UTL sera chiffrée de bout en bout par des mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS27)	Lan Commutateurs, Serveur , UTL, Poste admin ,
21	Architecture et exploitation des SI	Les outils d'administration devront intégrer les protocoles SSL/TLS. Ces protocoles seront également appliqués pour les échanges entre les lecteurs et les UTL.	Administrateur, UTL, lecteurs
22	Architecture et exploitation des SI	Protection physique des lecteurs : Les têtes de lecture devront être équipées d'un système de détection d'intrusion et d'arrachage, leurs fixations devront être renforcées.	Lecteurs
23	Architecture et exploitation des SI	Sécuriser les BDD de type Oracle conformément aux PES	Serveur
24	Architecture et exploitation des SI	Procéder au cloisonnement des ressources serveurs dans une DMZ dédiée à cet effet	Serveur
25	Gestion des autorisations ou accès logique aux ressources	Restreindre l'accès aux interfaces d'administration aux seuls administrateurs explicitement identifiés et authentifiés (ex : filtrage réseau, FW,...)	Serveur, UTL, postes administrateur, commutateurs
26	Gestion des autorisations ou accès logique aux ressources	Interdire l'accès aux fichiers de données aux prestataires Créer des comptes nominatifs pour les prestataires. Ces comptes devront être supprimés dès la fin de la prestation (cf procédure circuit arrivée/départ)	Serveur, postes administrateurs
27	Gestion des autorisations ou accès logique aux ressources	Journalisation des opérations réalisées par les administrateurs et installateurs Journalisation des actions sur le système de contrôle d'accès (création de badge, ouverture d'autorisation d'accès à des locaux, création d'utilisateurs dans la BDD, ...)	Serveur, postes admin
28	Gestion des autorisations ou accès logique aux ressources	Prévoir des badges temporaires ainsi qu'une procédure ad-hoc de délivrance et restitution de ces badges	Badges utilisateurs
29	Gestion des autorisations ou accès logique aux ressources	Utilisation de comptes nominatifs et de la carte agent pour l'authentification des administrateurs. Les comptes nominatifs des prestataires devront être activés/désactivés suivant les besoins d'intervention (cf procédure spécifique comptes nominatifs prestataires)	Administrateur
30	Gestion des autorisations ou accès logique aux ressources	Renouvellement des clefs et procédures de plusieurs porteurs Les clés sont classées par niveau de sensibilité. Idéalement les clés les plus sensibles (clé de lecture,etc.) sont réparties sur plusieurs porteurs Le système prévoit une gestion de renouvellement de clés minimisant les impacts fonctionnels	Badges utilisateur, badges administrateur

31	Gestion de la continuité des SI	En cas fonctionnement en mode dégradé (coupure électrique ou interruption des serveurs/UTL): garde statique, ouverture des accès stratégiques par clefs	Lecteurs, Lan, Commutateurs, Serveur UTL, Système de verrouillage
32	Gestion de la continuité des SI	Assurer la continuité de la fonction administration du SI : gestion des congés, astreintes,	Équipes admin
33	Gestion de la continuité des SI	Rédiger des fiches réflexes à appliquer en cas d'activation du plan de reprise d'activité (PRA) - S'assurer que les logiciels listés dans les fiches réflexes soient disponibles	Serveur
34	Gestion de la continuité des SI	S'assurer de la disponibilité des matériels listés dans les fiches réflexes : (plate-forme de secours, ...),	Serveur
35	Gestion de la continuité des SI	Prévoir un stock de maintenance pour les commutateurs	Lan, Commutateurs
36	Conformité et contrôle	Respect du « document de référence technique puce sans contact » rédigé par le SHFD	Lecteurs, Badges admin, Serveur, UTL, badges utilisateurs

16 DÉPOSE ET REMPLACEMENT DES ÉQUIPEMENTS

16.1 DÉPOSE

Le titulaire devra procéder à la dépose des équipements existants devenus obsolètes ou remplacés dans le cadre du présent marché. Cette prestation comprendra l'ensemble des opérations nécessaires à la mise hors service, au démontage et à l'évacuation des matériels concernés.

À ce titre, les éléments suivants devront être déposés :

- les enregistreurs existant, ainsi que les anciens postes d'exploitations et de visualisations vidéo, incluant les écrans associés;
- l'ensemble des switches dédiés à la vidéoprotection qui ne sont pas raccordés au réseau du ministère;
- toutes les caméras faisant l'objet d'un remplacement dans le cadre du présent projet;
- toutes les anciens lecteurs et coffrets objets d'un remplacement dans le cadre du présent projet;
- les blocs d'alimentation 230V associés aux équipements déposés.

Pour les caméras intérieures et extérieures : les coffrets, le câblage ainsi que leurs protections existants seront intégralement à démonter et remplacer. Idéalement, le nouveau câblage devra être tiré depuis l'intérieur des bâtiments, avec réalisation des percements nécessaires, afin d'éviter tout cheminement en extérieur, comme c'est actuellement le cas. Toutefois, dans les situations où un cheminement en apparent s'avérerait indispensable, les câbles devront être protégés conformément aux règles de l'art du ministère, notamment au moyen de protections métalliques de type Omega. Dans ce contexte, le tracé devra impérativement faire l'objet d'une validation préalable par les services de l'administration, notamment pour les façades classées.

Le titulaire veillera à réaliser ces opérations dans le respect des règles de sécurité, sans dégradation des infrastructures existantes.

16.2 STOCKAGE

Un local fermant à clé sera mis à disposition du titulaire par l'administration. Son emplacement sera défini lors de la visite de site en accord avec le

responsable du service immobilier du site. Ce local permettra d'entreposer le matériel en attente d'installation ainsi que tout élément démonté.

16.3 RECYCLAGE

Possibilité 1 : Recyclage par le soumissionnaire

Le soumissionnaire sera en charge d'évacuer tout le matériel démonté et de le rapatrier sur un centre de recyclage agréé.

Possibilité 2 : Recyclage par l'administration

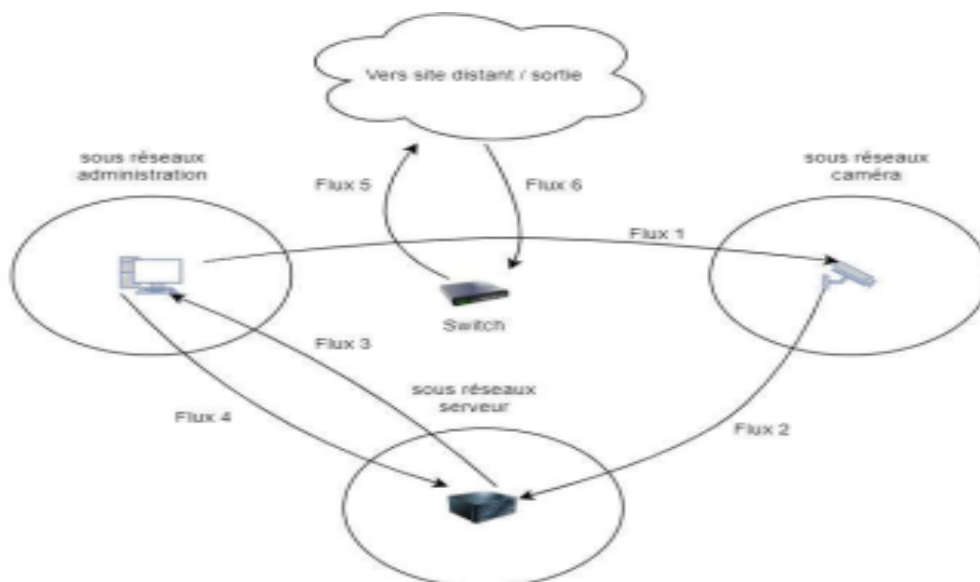
Tout le matériel démonté sera stocké dans un local indiqué par l'administration qui se chargera de le recycler.

Une exception sera faite pour tout élément contenant des données sensibles (disque dur, etc.). Les disques durs ne peuvent en aucun cas quitter le périmètre du site et seront remis à l'administration qui se chargera de les détruire. Aucune donnée ne peut être dupliquée sur tout support hors du site conformément aux recommandations SSI.

17 EXEMPLES DES ATTENDUS

17.1 EXEMPLE D'UN DIAGRAMME ET D'UNE MATRICE DE FLUX

Exemple pour une solution de vidéosurveillance :



Flux 1 : 192.168.0.1 vers 192.168.1.1 en 80/tcp, 80/UDP
Flux 2 : 192.168.1.1 vers 192.168.2.1 en 8080/UDP
Flux 3 : 192.168.2.1 vers 192.168.0.1 en 3389/TCP, 3389/UDP, 123/TCP, 161/TCP
Flux 4 : 192.168.0.1 vers 192.168.2.1 en 123/TCP, 67/UDP, 68/UDP, 135/TCP, 53/UDP
Flux 5 : 192.168.3.1 vers 172.16.0.1 en 69/TCP, 162/UDP, 123/TCP
Flux 6 : 172.16.0.1 vers 192.168.3.1 en 22/TCP, 69/TCP

Afin de réaliser un diagramme de flux réseaux, il faut prendre en compte tous les tenants et aboutissants de la solution. En effet, vous devez lister un par un les équipements qui devront communiquer sur le réseau après les avoir répartis par type en amont. Vous devez vous référer aux documentations techniques constructeurs et en extraire seulement les protocoles et ports utiles à la solution.

Vous relierez ceux-ci les équipements entre eux selon les flux nécessaires.

Exemple :

sous réseau administration

PC	192.16 8.0.1
----	-----------------

sous réseau
caméra

caméra	192.16 8.1.1
--------	-----------------

sous réseau
serveur

serveur switch	192.16 8.2.1
-------------------	-----------------

Switch-1
192.168.3.1

Protocoles numéro mode :

NTP 123 TCP

HTTP 80 TCP

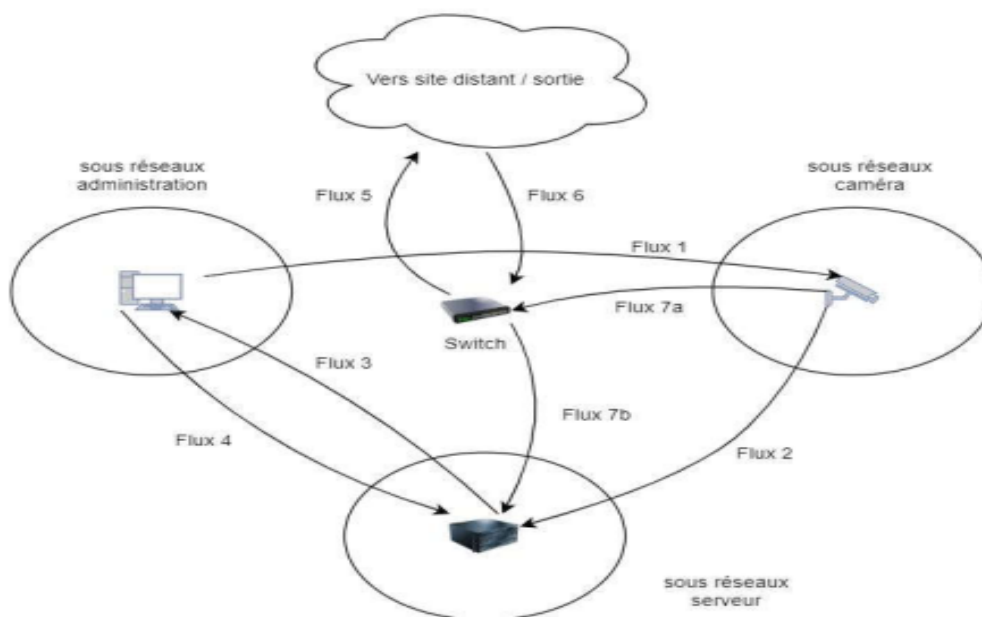
SNMP 161 UDP

RDP 3389 TCP/UDP

... ..

Les équipements de même type par constructeur pourront être représentés que par une seule icône. Un flux allant d'un équipement à un autre via un équipement de commutation sera désigné par Xa Xb.

Exemple :



Pour la formalisation littérale de ces flux, pour chacun d'eux appliquer la formule suivante :

- Flux [numéro] : [de l'adresse IP source] vers [l'adresse IP destination] en [numéro port] / [mode de connexion].

Exemple :

Flux 1 : 192.168.0.1 vers 192.168.1.1 en 80/TCP, 80/UDP

Ce qui donne une fois tous les flux référencés :

Flux 1 : 192.168.0.1 vers 192.168.1.1 en 80/tcp, 80/UDP

Flux 2 : 192.168.1.1 vers 192.168.2.1 en 8080/UDP

Flux 3 : 192.168.2.1 vers 192.168.0.1 en 3389/TCP,3389/UDP,123/TCP,161/TCP

Flux 4 : 192.168.0.1 vers 192.168.2.1 en 123/TCP, 67/UDP,68/UDP,135/TCP,53/UDP

Flux 5 : 192.168.3.1 vers 172.16.0.1 en 69/TCP,162/UDP,123/TCP

Flux 6 : 172.16.0.1 vers 192.168.3.1 en 22/TCP,69/TCP

Flux 7a,7b : 192.168.1.1 vers 192.168.2.1 en 1812/TCP,1813/TCP

Le soumissionnaire effectuera le même traitement pour les métiers du contrôle d'accès et de l'anti-intrusion. Il transmettra l'étude globale au chef de projet du SGAMI.

17.2 PROPOSITION DE PLAN D'UNE ANALYSE FONCTIONNELLE D'UNE SOLUTION DE SÛRETÉ BATIMENTAIRE.

I Cadre réglementaire et recommandations

Livrables de la configuration atelier intégrateur

II Synthèse du périmètre projet

III Système d'information

- A Infrastructure informatique
 - A1 Serveurs physiques
 - A2 Rôle Microsoft Windows Serveur
 - A3 Fonctionnalité Microsoft Windows
 - A4 Base de données – Sql Express
 - A5 Synchronisation horaire
 - A6 Agrégation des logs – Graylog
 - A7 Poste client
- B Infrastructure réseau
 - B1 Architecture logique
 - B2 Routage
 - B3 Configuration port d'accès
 - B4 Contrôle d'accès réseau
 - B5 Gestion des boucles réseau - Spanning Tree
 - B6 Lien vers l'extérieur
- C Haute disponibilité / tolérance aux pannes
 - C1 Enregistrement des flux vidéo
 - C2 Réplication synchrone de machines Hyper-V / Basculement
 - C3 Haute disponibilité des services Active Directory du domaine ..SURETE.LOCAL
 - C5 Interruption de service
 - C6 Fonctions Split Brain et VM Checker du logiciel de basculement

D Logiciel Vidéo

D1 Préambule

- D2 Localisation et distribution des services du VMS
- D3 Fonctionnalités déployées / configurées
 - D3.1 Communication sécurisée Client / Serveur
 - D3.2 Chiffrements et signature des enregistrements
 - D3.3 Communications sécurisées Caméra / Serveur
- D4 Organisation des groupes dans le VMS
 - D4.1 Groupe de caméra
 - D4.2 Groupe de microphone
 - D4.3 Groupe de haut-parleurs
 - D4.4 Groupe de Métadonnées
 - D4.5 Groupe des Entrées
 - D4.6 Groupe des Sorties
- D5 Groupe de vues
- D6 Les vues
 - D6.1 Vidéo
 - D6.2 Matrice (écran d'alarme)
- D7 Les alarmes de détection d'intrusion (périmétrie)
 - D7.1 Notification
 - D7.2 Secteurs et caméras associés
 - D7.3 Acquittements de l'alarme
- D8 Les rôles et utilisateurs
- D9 Les règles
- D10 Monitoring du système vidéo
 - D10.1 Serveur
 - D10.2 Caméras
 - D10.3 Disques
 - D10.4 Stockages
- D11 Préposition des dômes PTZ

E Logiciel d'analyse d'image –

E1 Analyse type Intrusion

- E1.1..... Scénarii d'intrusion
- E1.2..... Zones d'intrusion

F Centrale intrusion

F1 Secteurs

F1.1 Bâtiment A...

F1.2 jusqu'à Bâtiment N..

F1.3 Périmétries

F2 Zones

F3 Utilisateurs et droits

F3.1 Groupes

F3.2 Utilisateurs

F4 Mise en et hors service

F4.1 MES / MHS :

F4.2 Dérogations

F4.3 Point d'entrée / Point de sortie

F5 Connexion Ethernet

F6 Télésurveillance

F7 Lien avec le VMS

À l'issue de l'analyse fonctionnelle, le soumissionnaire écrira et programmera les scénarios d'asservissement des caméras aux ouvrants contrôlés par le contrôle d'accès dans la limite de deux scénarios en moyenne par ouvrants.

17.3 EXEMPLES DE SCENARIOS D'ASSERVISSEMENTS

1^{er} exemple :

Création de drapeaux, ou pointeurs, ou icônes dans la time line digitale de la solution globale au niveau de l'hyperviseur (affichage écran.)

Ces drapeaux signalent un événement avec un code couleur pour savoir si celui-ci a été acquitté par l'opérateur.
Exemple de time line classique : le curseur d'enregistrement avec multiflèches d'un magnétoscope.

Dans cet exemple : un drapeau = un événement

2^{ème} exemple :

Association de séquence vidéos courte de levée de doute sur pré-alarme ou post-alarme sur événement en temps réel.

Une séquence vidéo d'une trentaine de secondes (max mais possibilité moins) est associée via une icône dans le fil de l'eau des alarmes au niveau de l'hyperviseur.

L'opérateur quitte son poste pour une raison quelconque. Pendant son absence, un événement se produit générant une alarme qui s'affiche dans le fil de l'eau.

A son retour, il appuie sur l'icône apparaissant sur la ligne de l'alarme, ce qui a pour effet de lancer un pop-up affichant la séquence vidéo, pendant 30s, de la caméra associée afin de lever le doute. La séquence affichée peut-être pré ou poste alarme. Ne peut-être utilisée que sur un poste de gestion ou un agent est présent 24 h/24 ou 7j/7 ou bien encore hors heures ouvrables (cad avec présence durable de l'opérateur).

3^{ème} exemple :

Scénarios de préposition de dôme PTZ de levée de doute, en cas de présence de ce type d'équipement dans la solution (scénarios génériques).

Ces scénarios trouvent leurs origines dans l'expression de besoins des opérateurs ou des utilisateurs de la solution. Il faut donc qu'ils se la soient appropriés au travers de la présentation qui leur en sera faite grâce à l'analyse fonctionnelle.

En résumé, l'intégrateur doit expliciter dans l'analyse fonctionnelle clairement en langage simple les différentes actions programmées dans chaque scénario (qui peuvent être génériques) souhaitées par les utilisateurs de la solution.

17.4 IMPLANTATION TYPE BAIE DU RÉPARTITEUR ET/OU SOUS-REPARTITEUR

HAUT		
	U	ÉLÉMENT
2U	42	Panneau télécom (opérateur)
	41	Passe cordons télécom
	40	Panneau sûreté 24 noyaux RJ45
	39	Passe cordons
	38	Commutateur sûreté 24 ports POE
	37	Passe cordons
2U	36	Pare-feu

	35	sûreté
		Vide
		Vide
		Vide
		Vide
		Vide
2U	18	KVM
	17	
	15	Vide
	14	Vide
	13	Vide
	12	Vide
	11	Vide
	10	Vide
	9	Vide
	8	Serveur solution vidéo et contrôle d'accès
	7	
	6	Vide
	5	
	4	Onduleur sûreté
	3	
	2	Bandeau arrière 6 PC 220v+T sur onduleur
	1	Bandeau arrière 6 PC 220v+T
BAS		

18 DOCUMENTATION

18.1 DOCUMENTATION TECHNIQUE

Le titulaire du marché devra mettre à disposition une documentation complète sur les systèmes mis en œuvre comprenant :

- Les documentations techniques en français des matériels installés (version électronique et papier),
- Le Dossier des Ouvrages Exécutés (D.O.E.) en trois exemplaires papier et version électronique comprenant :
 - L'emplacement de tous les équipements installés (caméras, détecteurs, UTL, postes clients),
 - Le cheminement des câbles posés (courant fort et faible),
 - Les plans mis à jour au format dwg et ou pdf.

Ce document devra revêtir le timbre « DIFFUSION RESTREINTE ».

Toutes les pièces constituant cette documentation seront fournies en français sous forme de fichier électronique lisibles à partir de logiciels libres et en format papier sous forme de classeur.

18.2 DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION

Le titulaire du marché devra mettre à disposition une documentation d'exploitation des différents systèmes mis en œuvre comprenant :

- Un manuel d'administration système et des applications,
- Un manuel d'exploitation de chaque système,
- Une procédure de reprise des activités du système couvrant notamment l'arrêt forcé des équipements, leur redémarrage sur incident,
- Les consignes de sécurité pour le bon usage de la solution.

La documentation sera en version française.

18.3 SAUVEGARDE ET RESTAURATION

Le titulaire du marché devra mettre à disposition une documentation sur les procédures de sauvegarde et restauration des données permettant :

- Une sauvegarde journalière, hebdomadaire,
- Une sauvegarde/restoration différentielle, incrémentielle et complète.

19 FORMATION

Les formations seront assurées par des animateurs de formation spécialisés et habitués à ces types de formation. Elles se dérouleront à temps plein sur le site du client.

L'objectif est, qu'à l'issue de la formation, les personnels soient pleinement opérationnels dans le domaine de travail qu'ils doivent assurer.

Les supports de cours seront fournis en langue française, au format papier et au format électronique lisible à partir de logiciels libres. Ils seront classifiés en «DIFFUSION RESTREINTE».

Le titulaire proposera le contenu ainsi que la durée et le nombre de sessions qui seront adaptées au nombre de participants dans chaque domaine (administrateurs et exploitants).

20 RECETTE

La réception de la prestation est conditionnée par la fourniture de la documentation détaillée des architectures et des systèmes installés (spécifications techniques, paramétrages, configuration et exploitation, plan de recollement, fiches réflexes, etc..).

La recette technique se compose d'un contrôle d'inventaire, d'un contrôle visuel et d'un contrôle fonctionnel.

La recette technique est l'opération qui doit permettre de garantir au maître d'ouvrage que l'installation est conforme :

- Au CCTP,
- Aux performances attendues,
- Aux normes et réglementations en vigueur,
- Au guide d'installation du constructeur pour l'obtention de la garantie,
- Aux règles de l'art.

20.1 RECETTE DE L'INFRASTRUCTURE RÉSEAU

20.1.1 LE CONTRÔLE VISUEL

Après un contrôle quantitatif et qualitatif des composants fournis, le contrôle visuel portera sur la qualité générale de la prestation. On vérifiera notamment :

- Le respect des contraintes d'environnement,
- La mise en œuvre des câbles,
- La fixation des éléments (baies, panneaux, prises, modules, supports, etc.),
- La mise à la terre des éléments,
- L'installation des éléments actifs,
- L'étiquetage et le repérage des différents éléments,
- L'aspect esthétique,
- Le rebouchage.

20.1.2 LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur le comportement du système installé et plus particulièrement sur son aptitude à supporter les applications telles que définies dans le présent document. Pour ce qui concerne le câblage, ce contrôle comprendra notamment, pour chaque liaison permanente (permanent link), la mesure des paramètres définis dans la norme ISO/IEC 11801 2ème édition 1er amendement.

La recette fonctionnelle comprend les tests et mesures effectués sur l'installation de manière exhaustive.

Tous ces résultats seront consignés dans le dossier de recette du pré-câblage au format électronique de type pdf.

20.1.2.1 TESTS DES LIAISONS CUIVRE

Les tests de mesures à effectuer auront pour objet de vérifier que chaque paire est conforme d'une part, au plan d'installation, et d'autre part, à la qualité de transmission exigée.

A ce titre, le contrôle devra s'assurer pour chaque paire :

- Du raccordement correct de chaque extrémité et de la continuité de chaque paire,
- Du respect des polarités et de l'absence de court-circuit entre les conducteurs,
- De l'isolement par rapport à la terre et aux autres conducteurs,
- De l'absence de désappairage,
- De la résistance en boucle,
- De l'exactitude de son identification par rapport aux plans d'installation.

Toutes les liaisons "cuivre" devront être testées en configuration "**Permanent Link**". Ces tests devront être conformes à la norme ISO/IEC 11801 Edition 2, le câblage conforme au standard EIA/TIA-568-B.

Chaque fiche de test devra au minimum indiquer :

- La date du test,
- L'identification du lien,
- L'affectation des paires (WIRE MAP),

- La longueur des paires,
- L'impédance,
- L'affectation des paires (WIRE MAP),
- La résistance de boucle (DC LOOP RESISTANCE),
- La perte par insertion (INSERTION LOSS),
- La paradiaphonie (NEXT et PS NEXT),
- La télédiaphonie (FEXT et PS FEXT),
- Le rapport Signal/Bruit (ACR et PS ACR / ELFEXT et PS ELFEXT),
- La perte par réflexion (RETURN LOSS),
- Le délai de propagation (PROPAGATION DELAY),
- L'écart de propagation (SKEW).

En outre, la copie du certificat d'étalonnage ou la preuve d'achat (pour un appareil de moins d'un an) du testeur devra accompagner le rapport de test final.

L'ensemble de ces tests est à la charge du titulaire.

20.1.2.2 TESTS DES LIAISONS OPTIQUES

Deux mesures, dans les deux sens et à des longueurs d'ondes différentes selon le tableau ci-dessous :

	Multimode		Monomode	
Longueur d'onde (Nm)	850	1300	1310	1550
Atténuation maximum (dB/Km)	3,5	1,5	1,0	1,0

Toutes les liaisons optiques devront être testées dans les deux sens à l'aide d'un réflectomètre FO (OTDR) suivant le standard ISO/IEC 14 763-3.

Ces mesures ont pour but de s'assurer qu'aucune anomalie n'est présente sur la liaison optique :

- Défaut de raccordement,
- Atténuation élevée,

- Début de cassure ou contrainte.
- Chaque fiche de test devra au minimum indiquer :
 - La date du test,
 - L'identification du lien,
 - La longueur de la fibre,
 - L'atténuation mesurée (ainsi que les valeurs de chaque connecteur),
 - La longueur d'onde pour le test,
 - La direction dans laquelle le test a été réalisé.

L'ensemble de ces tests est à la charge du titulaire.

20.2 RECETTE DU COURANT FORT

20.2.1 LE CONTRÔLE VISUEL

On vérifiera notamment :

- Le respect des contraintes d'environnement,
- Le cheminement des câbles,
- La mise en œuvre des câbles, fixation, connexion,
- La mise à la terre des éléments,
- L'étiquetage et le repérage,
- Le rebouchage.

20.2.2 LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur :

- Le comportement en fonctionnement normal,
- Le comportement de l'installation en mode dégradé : coupure de l'énergie et vérification de la continuité de service correspondant aux dimensionnements des onduleurs.

20.3 RECETTE DES DIFFÉRENTS SYSTÈMES

Chaque système : contrôle d'accès, intrusion, système vidéo, visiophonie, postes de travail, sera contrôlé et réceptionné indépendamment.

Toutes les exigences décrites dans le chapitre correspondant sont testées à partir d'un cahier de recette qui sera défini durant les travaux préparatoires. Le titulaire propose à l'administration le cahier de recette que l'administration fait compléter et valider.

Les contrôles sont réalisés en présence du représentant de l'administration notamment pour ce qui a trait aux performances des équipements (détecteur et caméras) qui peuvent être mesurées spécifiquement par des tests d'intrusion.

20.3.1 LE CONTRÔLE QUANTITATIF ET QUALITATIF

Chaque matériel fourni par le titulaire sera comptabilisé et ses caractéristiques comparées à l'offre initiale.

Le titulaire s'engage à ce que la solution livrée soit protégée contre les virus et les logiciels malveillants connus au jour de l'installation.

L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie.

20.3.2 LE CONTRÔLE FONCTIONNEL

Le contrôle fonctionnel portera sur le comportement du système installé.

La recette fonctionnelle comprend les tests effectués sur l'installation de manière exhaustive.

Tous ces résultats seront consignés dans le dossier de recette.

La recette sera effectuée par l'administration en présence du titulaire.

Le contrôle devra donc s'assurer :

- Du bon fonctionnement des caméras intérieures et extérieures,
- Du bon fonctionnement du système de détection d'intrusion,
- De la qualité de l'image obtenue,
- Des unités de gestions et lecteurs de badge,
- Du bon paramétrage et du bon fonctionnement des logiciels de gestion du système,
- Des fonctionnalités du système et d'enregistrement/relecture des communications,
- Des fonctionnalités de visualisation et d'automatisation des ouvertures.

20.4 PROCESS VERBAL DE RECETTE

Le procès-verbal de recette comportera le compte-rendu des contrôles visuel et fonctionnel.

Il sera composé de deux parties distinctes :

- Infrastructure,
- Systèmes de sécurisation.

La réception définitive des travaux ne sera prononcée qu'après l'exécution de l'ensemble des essais et contrôles du système de vidéo et après la fourniture d'un dossier technique complet comprenant en particulier la nomenclature des équipements, les plans de câblage et de raccordement, les notices d'exploitation et d'entretien.

Si le procès-verbal fait état de réserves motivées par des omissions ou des imperfections, le titulaire disposera d'un délai de **15 jours** à définir avec le maître d'ouvrage pour exécuter les travaux nécessaires. Passé ce délai, le maître d'ouvrage pourra se réserver le droit de faire exécuter les travaux par une autre entreprise, aux frais, risques et périls du titulaire défaillant.

20.5 LES FICHES DE RECETTE

Les fiches de recette, fournies par le titulaire et complétées par l'administration, comprennent :

- La méthodologie et les procédures de tests,
- La description des tests,
- Les procès verbaux.

Ces trois étapes sont définies en concertation avec le titulaire.

20.6 VABF

La vérification d'aptitude et de bon fonctionnement (VABF) porte sur le respect des spécifications du CCTP et des résultats des tests. La VABF sera conduite par le titulaire, un représentant de l'administration, assistée par la MOE.

La durée de la VABF est de 30 jours ouvrés à partir de la validation de la recette.

Un procès-verbal est établi par la maîtrise d'ouvrage pour la validation de la VABF, conjointement avec le titulaire, à l'issue des opérations de validation, et propose pour l'administration une décision qui mentionne selon les cas :

- La réception sans réserve valant constat d'aptitude et de bon fonctionnement,
- La réception avec réserves (ajournement),
- Le rejet.

Ce procès-verbal cosigné est transmis au pouvoir adjudicateur, qui notifie sa décision au titulaire dans un délai de **30 jours ouvrés**.

La décision d'ajournement prévoit le délai imparti au titulaire pour remédier aux dysfonctionnements constatés. A l'issue de ce délai, une nouvelle procédure de validation de la VABF sur site est mise en place. Suite à cette nouvelle procédure, si des dysfonctionnements sont constatés, il sera procédé au rejet définitif de la prestation. Dès lors, la résiliation du marché aux torts exclusifs du titulaire peut être prononcée.

La décision d'acceptation avec réserves fixe le délai de levée des réserves. A cette issue, il sera procédé à de nouvelles vérifications. Il sera alors établi un procès-verbal de levée de réserves. Le constat d'aptitude et de conformité technique est dès lors réputé acquis à la date de l'établissement du premier procès-verbal.

20.7 VSR

La période de vérification de service régulier (VSR) est d'une durée de 60 jours ouvrés à compter de la date de réception de la VABF; elle est reconductible une fois, en cas d'ajournement. Elle est destinée à vérifier le bon fonctionnement des systèmes de sécurité dans les conditions d'exploitation définies par l'administration, avec la qualité de service définie dans le CCTP.

En cas de dysfonctionnement, l'administration peut être amenée à prononcer des réserves. Le titulaire doit remédier à ces problèmes dans un délai de 15 jours ouvrés. Un procès-verbal de vérification de service régulier

est établi à l'issue de cette période de VSR, après correction des éventuels dysfonctionnements, et fourniture de l'ensemble des livrables.

A l'issue, en cas de dysfonctionnements toujours constatés, l'ajournement de l'admission peut être prononcé, avec mise en demeure de les corriger. En cas de carence du titulaire dans les délais impartis, il est procédé au rejet définitif de la solution. Le rejet n'est prononcé par l'administration qu'après constat contradictoire de ces dysfonctionnements. La résiliation du marché aux torts exclusifs du titulaire, ou la mise en régie aux frais et risques de ce dernier, peut dès lors être prononcée.

En tout état de cause, la réception définitive n'est effective qu'après constat de la livraison de l'ensemble des documents requis. Elle fait l'objet d'une décision expresse de l'administration, qui intervient au plus tard dans le délai de 15 jours ouvrés à compter du constat de levée de réserves ou de levée des motifs d'ajournement prononcés dans le cadre de cette VSR.

Elle est ensuite notifiée au titulaire.

20.8 RÉCEPTION DÉFINITIVE

La réception définitive de la solution n'est prononcée qu'après remise des documents permettant la prise en charge des installations par le Maître d'Ouvrage et au terme de la VSR.

Dans le cas où le Maître d'Ouvrage serait amené à prendre possession des installations sans la remise de ces documents, les installations sont exploitées suivant les instructions de l'entreprise et sous sa responsabilité, sans que cette dernière puisse prétendre à indemnisation.

21 GARANTIE

21.1 MODALITÉS

Le service demandeur doit préciser les actions à exécuter lors de la maintenance face à chaque type ou cas de panne.

La garantie débute à compter de la réception définitive de l'installation.

Elle comprend l'échange de pièces, la main d'œuvre et les déplacements, à l'exception des disques durs qui font l'objet d'un cas particulier.

Les disques durs remplacés ne peuvent en aucun cas quitter le périmètre du site et sont remis à un représentant du client (contre décharge si besoin). Aucune donnée ne peut être dupliquée sur tout support hors du site.

Durant la période de garantie, le titulaire s'engage à remplacer à l'identique, à réparer ou à modifier toutes les pièces ou éléments reconnus défectueux. Il doit corriger les erreurs constatées au sein des logiciels fournis.

Les modalités d'accès à la maintenance seront mises en place par le titulaire qui fournira la procédure de signalisation des dérangements.

Les incidents seront enregistrés sous forme de tickets numérotés qui indiqueront :

- L'identité et la localisation du demandeur,
- Le descriptif précis du dérangement,
- La date et l'heure de signalisation.

La télémaintenance est proscrite, si la résolution de l'incident n'est pas possible d'une manière simple et rapide par assistance téléphonique, le dépannage devra se faire par déplacement d'un technicien.

21.2 INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE

21.2.1 DÉFINITION DE LA GRAVITE DE L'INCIDENT

Deux niveaux de gravité d'incident sont définis :

1. Panne urgente:

Une panne urgente correspond à une panne rendant le système complètement inexploitable.

2. Panne non urgente:

Toutes les autres pannes sont considérées comme non urgentes.

21.2.2 GARANTIES DE TEMPS DE RÉTABLISSEMENT (GTR)

Panne urgente (option 1):

Elle devra être réparée dans les 4 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Panne urgente (option 2) :

Elle devra être réparée dans les 24 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Panne non urgente :

Elle devra être réparée dans les 48 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi).

Le début de la période prise en compte dans le cadre des garanties de rétablissement correspond aux date et heure de signalisation d'incident (ticket horodaté).

21.3 MISES A JOUR

Pendant la période de garantie, les mises à jour préconisées par le constructeur ou permettant de corriger une anomalie pourront être installées après accord préalable de l'administration.

Une procédure de mise à jour sera définie pour maintenir le service opérationnel (définition d'un plan de repli pendant la mise à jour, choix d'un moment propice dans la journée).

21.4 INTERVENTION APRÈS LA PÉRIODE DE GARANTIE

En plus de renseigner le CRT onglet GARANTIE & MAINTENANCE, **le titulaire fournira un contrat type de maintenance pour une mise à jour logicielle majeure annuelle détaillé et chiffré basé sur les éléments du système déployé.**

22 PLANS

Ils récapitulent les types et emplacements des périphériques relatifs au projet. Ils seront remis lors de la visite sur site, s'ils ont été établis (en fonction de la complexité du projet).

23 SYNOPTIQUES DU PROJET

Ils explicitent de manière graphique le fonctionnement, les types et emplacements des périphériques relatifs au projet. Ils seront remis lors de la visite sur site, s'ils ont été établis (en fonction de la complexité du projet).

24 DÉCOMPOSITION DU PRIX GLOBAL ET FORFAITAIRE

La Décomposition du Prix Global et Forfaitaire est à remplir obligatoirement et vient en complément de la réponse au CCTP.

Fichier de référence :

Prefecture_TULLE-Acces_et_Vidéo_2026_DPGF.xlsx

25 ANNEXES

25.1 ANNEXE 1 : PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT

**ANNEXE 1 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CÂBLAGE
ÉQUIPEMENTS RACCORDEMENT**

25.2 ANNEXE 2 : PRINCIPE CONTRÔLE D'ACCÈS

**ANNEXE 2 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES CONTRÔLE
ACCÈS**

25.3 ANNEXE 3 : NORMES ET RÉGLEMENTATIONS

**ANNEXE 3 - CCTP SÛRETÉ SGAMI DSIC_NORMES ET
RÉGLEMENTATIONS APPLICABLES**

25.4 ANNEXE 5 : PRINCIPE D'EXPLOITATION

**ANNEXE 5 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES
D'EXPLOITATION**

25.5 ANNEXE 6 : PRINCIPE VIDÉOPROTECTION

**ANNEXE 6 - CCTP SÛRETÉ SGAMI DSIC_PRINCIPES VIDÉO
PROTECTION 2024**

26 GLOSSAIRE

CCTP : Cahier des Clauses Particulières

CRT : Cadre de Réponse Technique

D.O.E.: Dossier des Ouvrages Exécutés

DPGF : Décomposition du Prix Global Forfaitaire

GAC : Gestion d'Accès Contrôlé (Désigne le logiciel de gestion du contrôle d'accès)

PSE : Prestation-s Supplémentaire-s Éventuelle-s

SRTP : Protocol Secure Real-Time Transport Protocol est une extension sécurisée du protocole RTP, offrant cryptage, authentification et protection contre les attaques pour les communications en temps réel.

VMS : Video Management System (Désigne le logiciel de gestion de vidéosurveillance)