

MARCHÉ PUBLIC DE FOURNITURES COURANTES ET DE SERVICES

Cadre juridique : article L.2125-1 du Code de la commande publique (accord-cadre)

Dispositions générales : articles R.2162-1 à R.2162-6 du Code de la commande

Dispositions propres aux bons de commande : articles R.2162-13 et R.2162-14 du Code de la commande publique

Prestations d'installation, fourniture, maintenance et mise en service de systèmes de sûreté électronique des services du ministère de l'Intérieur au sein des Services de l'État en Guyane et de la Direction territoriale de la Police Nationale de Guyane.

**CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES
(CCTP)**

Le présent document est complété par des annexes techniques dont les principes généraux seront à appliquer lors de l'établissement de votre offre et à respecter lors de la réalisation des prestations

Les annexes suivantes sont jointes au document :

- ANNEXE 1 - CCTP SÛRETÉ PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT
- ANNEXE 2 - CCTP SÛRETÉ PRINCIPES CONTRÔLE D'ACCÈS
- ANNEXE 3 - CCTP SÛRETÉ PRINCIPES DÉTECTION INTRUSION
- ANNEXE 4 - CCTP SÛRETÉ PRINCIPES VIDÉO PROTECTION
- ANNEXE 5 - CCTP SÛRETÉ PRINCIPES EXPLOITATION

Rappel des modalités :

Le titulaire doit obligatoirement être référencé et qualifié (certification constructeur et/ou attestation de formation) pour les matériels qu'il propose pour la sécurisation du site. De fait, le titulaire devra connaître les textes et prescriptions en vigueur.

Les prestations, services, matériels et installations doivent être conformes aux normes, règlements et décrets (éditions en vigueur à la date de signature du marché) et respecteront les règles de l'art applicables dans leur dernière édition complétée de leurs additifs.

De fait, le titulaire devra assurer une veille sur les normes, règlements et décrets

D'une manière générale, le titulaire du contrat doit respecter l'ensemble des textes réglementaires (lois, décrets, arrêtés, circulaires) et para-réglementaires (normes, document technique unifié (DTU) avis techniques et solutions techniques).

Table des matières

1 DESCRIPTION GÉNÉRALE DES PROJETS.....	6
1.1 OBJET DE LA CONSULTATION	6
1.2 LE BESOIN DU POUVOIR ADJUDICATEUR ET DES BENEFICIAIRES.....	6
1.3 DEVOIR DE CONSEIL DU TITULAIRE.....	6
1.4 PRESTATION P0 D'ÉTUDE DU BESOIN.....	6
1.5 LE DEVIS DE RÉALISATION	7
1.5.1 AVEC ÉTUDE.....	7
1.5.2 SANS ETUDE	8
1.6 EMISSION DE LA COMMANDE ET PLANNING PREVISIONNEL D'EXECUTION.....	8
1.7 LES PRESTATIONS DE RÉALISATION	8
1.7.1 PRÉAMBULE	8
1.7.1.1 DIAGNOSTICS MATÉRIAUX	8
1.7.1.2 INTERACTION AVEC D'AUTRE CORPS D'ÉTAT	8
1.7.1.3 DEVOIR DE CONSEIL DU TITULAIRE DURANT LA RÉALISATION.....	9
1.7.1.4 RÈGLES D'EXÉCUTION DES PRESTATIONS	9
1.7.1.5 DÉMARCHE QUALITÉ.....	9
1.7.2 PRESTATION P1 DE FOURNITURE, INSTALLATION, RACCORDEMENT ET MISE EN SERVICE D'UN SYSTÈME DE VIDÉO PROTECTION, DE CONTRÔLE D'ACCÈS, DE DÉTECTION D'INTRUSION, D'INTERPHONIE / VISIOPHONIE (PRIMO INSTALLATION)	10
1.7.2.1 les sous prestations.....	10
1.7.2.1.1 Condition d'exécution.....	11
1.7.2.1.2 Les attendus de la phase réalisation	11
1.7.2.1.3 les attendus de la phase de réception.....	12
1.7.2.1.4 les livrables attendus pour une ou plusieurs sous-prestation.....	12
1.7.3 PRESTATION P2 DE FOURNITURE, INSTALLATION, RACCORDEMENT ET MISE EN SERVICE D'UN SYSTÈME DE VIDÉO PROTECTION, DE CONTRÔLE D'ACCÈS, DE DÉTECTION D'INTRUSION, D'INTERPHONIE / VISIOPHONIE (EXTENSION D'UN SYSTÈME EXISTANT).....	14
1.7.3.1 les sous prestations.....	14
1.7.3.1.1 Condition d'exécution.....	14
1.7.3.1.2 Les attendus de la phase réalisation	15
1.7.3.1.3 les attendus de la phase de réception.....	15
1.7.3.1.4 les livrables attendus pour une ou plusieurs sous-prestation.....	16
1.7.4 PRESTATION P3 DE DÉMONTAGE/DÉPOSE	18
1.7.4.1 Démontage/dépose.....	18
1.7.4.2 Stockage	18
1.7.4.3 Recyclage.....	18
1.7.5 PRESTATION P4 DE FORMATION/TRANSFERT DE COMPETENCES.....	18
1.7.5.1 Formation des Administrateurs.....	19
1.7.5.2 Formation des Gestionnaires de badges.....	19
1.7.5.3 Formation des Exploitants/Opérateurs.....	19

1.7.6 PRESTATIONS DE MAINTENANCE ET D'EXPLOITATION DES SYSTEMES DE SURETE	20
1.7.6.1 Objet des prestations	20
1.7.6.2 Périmètre général de la maintenance.....	20
1.7.6.3 Typologie des prestations de maintenance.....	20
1.7.6.3.1 Maintenance préventive	20
1.7.6.3.2 Maintenance corrective	20
1.7.6.3.3 Maintenance évolutive et assistance à l'exploitation	21
1.7.6.4 Organisation et modalités d'intervention.....	21
1.7.6.5 Niveaux de service et engagements	21
1.7.6.6 Prestations de télésurveillance (optionnel).....	21
1.7.6.7 Traçabilité, reporting et documentation	21
1.7.6.8 indépendance technologique et pérennité	21
1.7.6.9 Modalités financières	22
1.7.6.10 Modalités de mise en œuvre dans le cadre d'un marché à bons de commande	22
1.7.6.11 Activation progressive et périmètre variable	22
5.12 Absence d'exclusivité et continuité de service	22
1.7.6.13 Cohérence avec les prestations d'installation, de mise en service et de maintenance	22
2 LES EXIGENCES ET SPÉCIFICITÉS DES SYSTÈMES	22
2.1 INFRASTRUCTURE RÉSEAU	22
2.1.1 LA DORSALE OPTIQUE.....	23
2.1.2 LE CAPILLAIRE CUIVRE.....	23
2.1.3 LES BAIES	23
2.1.4 LES ÉLÉMENTS ACTIFS.....	23
2.1.5 CÂBLAGE SPÉCIFIQUE SÛRETÉ BATIMENTAIRE	23
2.1.5.1 UTL contrôle d'accès.....	23
2.1.5.2 Lecteurs de badges	23
2.1.5.3 Caméras.....	24
2.1.5.4 Station de supervision et de gestion.....	24
2.1.5.5 Cordons de brassage.....	24
2.2 SYSTÈME DE CONTRÔLE D'ACCÈS.....	24
2.2.1 COMPATIBILITÉ.....	24
2.2.2 GÉNÉRALITÉS.....	24
2.2.3 SOLUTION DE CONTRÔLE D'ACCÈS CERTIFIÉE ANSSI.....	25
2.2.4 FOURNITURE ET POSE DES SERRURIES.....	25
2.2.5 OBSTACLES MÉCANIQUES.....	25
2.2.6 MAQUETTE ET CÉRÉMONIE DES CLÉS (USINE).....	25
2.3 SYSTÈME DE DÉTECTION INTRUSION	26
2.4 SYSTÈME DE VIDÉO-PROTECTION.....	26
2.5 CAS DE SOLUTION UNIFIÉE VIDEOPROTECTION ET CONTRÔLE D'ACCÈS.....	26
3 LES EXIGENCES DOCUMENTAIRES, D'ADMINISTRATION ET D'EXPLOITATION	26

3.1 DOCUMENTATIONS	26
3.1.1 DOCUMENTATION TECHNIQUE.....	26
3.1.2 DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION.....	27
3.1.3 SAUVEGARDE ET RESTAURATION	27
3.2 LA RÉCEPTION (VABF ET VSR)	27
3.2.1 VABF	27
3.2.1.1 Les recettes.....	28
3.2.1.1.1 Recette fonctionnelle.....	28
3.2.1.1.2 Recette câblage	28
3.2.1.1.3 Recette de Conformité au CCTP.....	30
3.2.1.1.4 Le contrôle quantitatif et qualitatif.....	30
3.2.2 VISITE DE VALIDATION D'APTITUDE	30
3.2.3 PROCÈS VERBAL DE VALIDATION D'APTITUDE.....	31
3.2.4 AJOURNEMENT	31
3.2.5 VSR.....	31
3.2.6 RÉCEPTION DÉFINITIVE.....	32
3.3 GARANTIE	32
3.3.1 MODALITÉS.....	32
3.3.2 INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE.....	32
3.3.2.1 Astreinte téléphonique	32
3.3.2.2 Définition de la gravité de l'incident	32
3.3.2.3 Garanties de temps de rétablissement (GTR).....	33
3.3.3 MISES À JOUR.....	33
4 LES EXIGENCES SSI.....	33
Principes de Sécurité des Systèmes d'Information	33

1 DESCRIPTION GÉNÉRALE DES PROJETS

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 création, la rénovation et l'extension d'installations existantes dans les domaines

- de vidéo-protection
- de contrôle d'accès
- de détection d'intrusion
- d'interphonie et visiophonie

1.2 LE BESOIN DU POUVOIR ADJUDICATEUR ET DES BENEFICIAIRES

Le besoin des Services de l'Etat en Guyane (SEG) , représenté par la Direction des Systèmes d'Information (DSI) est exprimé au travers d'une expression de besoin détaillée de sûreté électronique (périmètres et fonctionnalités attendues) accompagnée de plans des bâtiments à l'échelle (format « dwg ou pdf ») ainsi que tout autre documents nécessaires à la réalisation, par le titulaire, de l'étude. Il pourra être porté à la connaissance du titulaire tout diagnostic pouvant influencer une éventuelle réalisation (ex diagnostic amiante).

Cette expression de besoin est obligatoire et préalable à ce qui suit.

1.3 DEVOIR DE CONSEIL DU TITULAIRE

Le titulaire est expert dans les solutions de sûreté électronique, aussi en tant que titulaire du marché, il a un devoir de conseil et d'expertise. Il doit alerter et conseiller le pouvoir adjudicateur et, le cas échéant, le bénéficiaire sur les problématiques qui peuvent être décelées ou rencontrées. Ce devoir n'est pas une prestation facturable.

Ainsi, selon l'expression du besoin exprimé, le titulaire vérifiera, dans la mesure du possible, les capacités du système en place à répondre au besoin exprimé sans étude préalable. Le titulaire communiquera son conseil détaillé par mail au chargé de projet sûreté bâtiminaire de la DSI.

1.4 PRESTATION P0 D'ÉTUDE DU BESOIN

L'étude est obligatoire pour toute demande complexe qui impacterait le système existant d'un point de vue logicielle, infrastructure, solution de sûreté ou dans le cadre d'une primo installation (cf §1.3).

Elle peut correspondre à un ou plusieurs domaines. Un domaine correspond à

- vidéoprotection
- contrôle d'accès
- détection d'intrusion
- interphonie/visiophonie

L'étude comprend :

- une visite de site (CCAP sûreté électronique 7.1.1) pour le partage et la compréhension du besoin
- la retranscription de l'étude dans un mémoire technique correspondant au dimensionnement du projet au besoin exprimé, dans le respect des annexes techniques jointes au CCTP
=> le mémoire technique inclura obligatoirement le détail du métrage câblage => 30 pages maximum par domaine
- une estimation financière représentative du besoin exprimé sur la base du BPU en vigueur
- la restitution en visio ou sur site (durée estimée 2h) du mémoire technique

NB : dans le cadre d'une modernisation ou d'une extension, le titulaire proposera dans la mesure du possible la réutilisation du matériel et des licences acquises et vérifiera les capacités du système existant à évoluer et accueillir de nouveaux dispositifs dans le cadre d'extension.

La prise de rendez-vous pour une visite de site sera à l'initiative du bénéficiaire ou du pouvoir adjudicateur par un moyen tracé (mail ou courrier) et la visite devra avoir lieu au maximum 4 semaines après la demande écrite.

Le mémoire technique détaillé permet d'expliquer le devis, la solution et l'organisation du chantier.

Il contiendra :

- Une présentation de la solution et de son architecture
- Une présentation des fonctionnalités de la solution
- Le calendrier prévisionnel de la réalisation à la réception sur la base d'une date T0
- Les modalités du suivi de chantier (réunion de suivi, reporting, réunion de préparation de chantier, ...) Le tableau des ouvriers pour le contrôle d'accès
- L'étude DORI pour chaque caméra
- La stratégie de bascule/migration en cas de remplacement d'un système existant
- Le système de sauvegarde qui sera mis en œuvre
- Les contrôles qualité qui seront menés tout au long du chantier
- Les tests qui seront réalisés pour valider le bon fonctionnement
- Listes des contraintes projet prises en compte (amiante, bâtiment de France, air salin, sur le parcours des manifestations ...)
- Les formations envisagées
- Modalités d'interaction avec d'autres corps d'état (menuisier, plaquiste, peintre, électriciens)
- Le rappel de la documentation qui sera remise en fin de chantier et exigée au titre du CCTP
- Les garanties sur le matériel et installateur
- en annexe, les plans avec les emplacements des différents équipements et les cônes de visualisation pour les caméras

Les livrables attendus sont les suivants :

Nom du livrable	Délai de production (titulaire)	Délai de validation (bénéficiaire/pouvoir adjudicateur)
Mémoire technique et Estimation financière	15 jours calendaires après la visite de site	15 jours calendaires après la livraison du document

Le pouvoir adjudicateur, après recueil auprès du bénéficiaire le cas échéant, validera le mémoire technique permettant ainsi au titulaire de délivrer un devis de réalisation.

1.5 LE DEVIS DE RÉALISATION

1.5.1 AVEC ÉTUDE

Le devis est à délivrer selon les conditions ci-dessous :

Nom du livrable	Délai de production (titulaire)	Délai de validation (bénéficiaire/pouvoir adjudicateur)
Devis	15 jours calendaires après la validation du mémoire technique	15 jours calendaires après la livraison
Actualisation Devis	3 jours ouvrés à réception de la demande de modification (sur erreur ou ajout)	5 jours ouvrés à réception du devis rectificatif

Le devis aura, sauf modification du BPU par avenant, une durée de validité fixée à 60 jours minimum à partir de la date d'émission (durée à inscrire sur le devis).

Dans le cas d'une référence hors catalogue, le devis devra intégrer le pourcentage de remise indiqué dans le BPU.

1.5.2 SANS ETUDE

Une visite de site pour le partage et la compréhension du besoin est obligatoire. Il s'agira principalement de fourniture/installation/mise en service sur un système existant sans impact logiciel, infrastructure ou solution de sûreté.

La prise de rendez-vous pour une visite de site sera à l'initiative du bénéficiaire par un moyen tracé (mail ou courrier) et la visite devra avoir lieu au maximum 4 semaines après la demande écrite. Le devis est à délivrer selon les conditions ci-dessous :

Nom du livrable	Délai de production (titulaire)	Délai de validation (bénéficiaire)
Devis	15 jours calendaires après la visite de site	15 jours calendaires après la livraison
Actualisation Devis	3 jours ouvrés à réception de la demande de modification (sur erreur ou ajout)	5 jours ouvrés à réception du devis rectificatif

Le devis aura, sauf modification du BPU par avenant, une durée de validité fixée à 60 jours minimum à partir de la date d'émission (durée à inscrire sur le devis).

Sur le plan documentaire, il est demandé dans ce cadre la livraison de :

- Un plan d'implémentation et de câblage
- Le tableau des ouvrants dans le cas du contrôle des accès
- Un planning d'exécution des prestations - Un annuaire de contact identifié

1.6 EMISSION DE LA COMMANDE ET PLANNING PREVISIONNEL D'EXECUTION

La commande est émise sur la base du devis validé par le pouvoir adjudicateur ou le bénéficiaire et transmise en format dématérialisé.

Le titulaire, à réception de la commande (date figurant sur le bon de commande CHORUS faisant foi), dispose d'un délai de 10 jours ouvrés ou au plus tard 20 jours ouvrés avant le début des prestations pour communiquer un plan d'exécution des prestations incluant à minima:

- un planning prévisionnel pour l'exécution des prestations avec identification obligatoire des contraintes/jalons/dépendances de réalisation,
- un plan d'implémentation matériel, de réservation cheminement et de câblage,
- un annuaire de contact (nom/prénom/fonction/téléphone et email nominatif)
- tout autre élément nécessaire à l'exécution des prestations

Nom du livrable	Délai de production (titulaire)
Plan d'exécution des prestations	10 jours ouvrés après réception de la commande ou au plus tard 20 jours ouvrés avant le début des prestations

1.7 LES PRESTATIONS DE RÉALISATION

1.7.1 PRÉAMBULE

1.7.1.1 DIAGNOSTICS MATÉRIAUX

Si nécessaire les Dossiers Techniques Amiante (DTA) et Diagnostics Amiante Avant Travaux (DAAT) seront fournis par le pouvoir adjudicateur ou le bénéficiaire selon le cas.

1.7.1.2 INTERACTION AVEC D'AUTRE CORPS D'ÉTAT

Les prestations demandés dans le cadre du présent marché peuvent s'inscrire dans un chantier plus large immobilier, la synchronisation avec d'autres corps d'état (menuisier, peintre, électricien etc.) ainsi que le partage de la documentation pour le bon déroulement du chantier global sont essentiels. Les mémoires techniques, devis,

réalisation doivent tenir compte de cette composante. Le rôle de conseil, coordination du titulaire et le dialogue sont importants dans ce cadre, ce, pour toutes les phases.

1.7.1.3 DEVOIR DE CONSEIL DU TITULAIRE DURANT LA RÉALISATION

Le titulaire est expert dans les solutions de sûreté électronique, aussi en tant que titulaire du marché, il a un devoir de conseil et d'expertise. Il doit alerter et conseiller le pouvoir adjudicateur ou le bénéficiaire sur les problématiques qui peuvent être décelées ou rencontrées lors de l'exécution des prestations. Ce devoir n'est pas une prestation facturable.

1.7.1.4 RÈGLES D'EXÉCUTION DES PRESTATIONS

Les systèmes sont prévus pour apporter une solution de sécurité 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. Le périmètre de sécurité comprend, outre l'intérieur des bâtiments, l'étendue des sites ainsi que leurs abords limitrophes.

Les prestations s'exécutent conformément aux exigences et spécificités décrites dans ce document (LES EXIGENCES ET SPÉCIFICITÉS DES SYSTÈMES, LES EXIGENCES DOCUMENTAIRES, D'ADMINISTRATION ET D'EXPLOITATION et LES EXIGENCES SSI) ainsi que dans ses annexes :

- ANNEXE 1 - CCTP SÛRETÉ PRINCIPES CÂBLAGE ÉQUIPEMENTS RACCORDEMENT
- ANNEXE 2 - CCTP SÛRETÉ PRINCIPES CONTRÔLE ACCÈS
- ANNEXE 3 - CCTP SÛRETÉ PRINCIPES DÉTECTION INTRUSION
- ANNEXE 4 - CCTP SÛRETÉ PRINCIPES VIDÉO PROTECTION
- ANNEXE 5 - CCTP SÛRETÉ PRINCIPES EXPLOITATION

Les prestations, services, matériels et installations doivent être conformes aux normes, règlements et décrets (éditions en vigueur à la date de signature du marché) et respecteront les règles de l'art applicables dans leur dernière édition complétée de leurs additifs.

Les documents de référence sont des documents pouvant être utilement consultés pour élaborer les offres et projets de contrat ainsi que pour l'exécution du contrat.

D'une manière générale, le titulaire doit respecter l'ensemble des textes réglementaires - lois, décrets, arrêtés, circulaires - et para-réglementaires - normes, document technique unifié (DTU), avis techniques et solutions techniques.

Le titulaire est tenu d'informer l'administration de toute discordance entre le CCTP et les règles énoncées ou non dans la législation, ainsi que de toutes les questions qui pourraient être une source de litige par la suite.

Les choix techniques découlent directement des besoins fonctionnels exprimés, des objectifs en termes d'évolution et des contraintes d'environnement.

Le marché prévoit:

- La fourniture, installation, raccordement et mise en service d'un système de vidéo protection de contrôle d'accès de détection d'intrusion, d'interphonie / visiophonie (câblage courants forts et faibles, éléments matériels actifs, passifs, logiciels et licences) dans le cadre d'une primo installation ou d'une extension,
- La fourniture de la documentation des ouvrages exécutés, d'administration et d'exploitation nécessaire au maintien en condition des systèmes,
- La formation des personnels chargés de la gestion et l'exploitation du système mis en œuvre,
- La garantie sur le matériel et les logiciels livré,
- La dépose, le stockage et/ou enlèvement du matériel obsolète.

1.7.1.5 DÉMARCHE QUALITÉ

Le titulaire devra s'organiser afin de s'inscrire dans une démarche qualité interne.
Cette démarche vise à :

- Établir les modèles des différents livrables attendus qui n'auraient pas été fournis par le pouvoir adjudicateur
- Établir la liste des vérifications, contrôles qualité qui seront réalisés systématiquement en interne pour chaque projet
- Vérifier la qualité de la documentation livrée pour chaque projet
- S'assurer que les mêmes standards de prestation seront appliqués à chaque projet par les différentes équipes et intervenants
- S'assurer que les mêmes modèles de documentation seront appliqués à tous les projets
- Formaliser et partager un retour d'expérience pour chaque projet qui le nécessite
- Proposer des ajustements/adaptations en fonction des retours d'expérience sur les projets
- Appliquer ces ajustements/adaptations à l'ensemble des nouveaux projets. La démarche sera annexée à chaque mémoire technique livré.

1.7.2 PRESTATION P1 DE FOURNITURE, INSTALLATION, RACCORDEMENT ET MISE EN SERVICE D'UN SYSTÈME DE VIDÉO PROTECTION, DE CONTRÔLE D'ACCÈS, DE DÉTECTION D'INTRUSION, D'INTERPHONIE / VISIOPHONIE (PRIMO INSTALLATION)

Le titulaire devra se référer à chaque annexe correspondante pour les conditions techniques de réalisation. Un chantier pourra intégrer une ou plusieurs sous-prestations selon le besoin.

1.7.2.1 les sous prestations

- SP1.1 Fourniture, installation, raccordement et mise en service d'un système de vidéo protection,
- SP1.2 Fourniture, installation, raccordement et mise en service d'un système de contrôle d'accès,
- SP1.3 Fourniture, installation, raccordement et mise en service d'un système de détection d'intrusion,
- SP1.4 Fourniture, installation, raccordement et mise en service d'un système d'interphonie / visiophonie

Chaque sous-prestation est considérée comme un ensemble indivisible de prestations constituant le socle de fourniture et d'installation d'un système de sûreté électronique opérationnel.

Le socle de prestation comprend, de manière non exhaustive, l'ensemble des actions, opérations et livrables nécessaires à la livraison d'une solution complète, fonctionnelle, conforme aux exigences du présent CCTP, à l'exclusion uniquement :

- de l'acquisition des matériels unitaires,
- des licences logicielles,
- de la dépose d'un existant,
- de la formation des utilisateurs,
- et de la pose du câblage.

Font notamment partie intégrante du socle, sans pouvoir donner lieu à une facturation distincte :

- la pose, le raccordement, le paramétrage et l'intégration des équipements de sûreté électronique, qu'ils soient existants ou nouvellement acquis ;
- les réglages fonctionnels, la configuration logicielle, les interconnexions et les tests de bon fonctionnement ;
- la réalisation de l'ensemble des essais, tests techniques et fonctionnels, ainsi que des opérations de recette (interne et contradictoire) ;
- la mise en service complète du système, incluant la vérification de la conformité aux exigences fonctionnelles, techniques et réglementaires.

La documentation et les livrables contractuels font partie intégrante du socle de prestation.
À ce titre, le titulaire devra fournir, au minimum, un Dossier des Ouvrages Exécutés (DOE) comprenant notamment :

- les plans et schémas « tel que construit » (synoptiques, architectures, implantations) ;
- les schémas de câblage et de raccordement ;
- les configurations et paramétrages des équipements et logiciels ;
- les notices d'exploitation et de maintenance ;
- les procès-verbaux de tests, essais et recettes ;
- toute documentation nécessaire à l'exploitation, à la maintenance et à l'évolution ultérieure du système.

La fourniture complète et conforme de ces livrables conditionne la réception des prestations.

Le BPU mentionne des tranches considérant :

- « porte » comme un ensemble d'éléments permettant de la sécuriser (par ex l'association de lecteurs de badge en entrée et possiblement en sortie, d'une serrure, d'une ventouse, d'un BG vert ou d'un bouton sortie, un possible asservissement à la centrale incendie ...) y compris le système informatique associé Une sécurisation correspond a minima à un lecteur de badge de contrôle d'accès.
- « caméra » comme un ensemble d'élément vidéo y compris le système informatique associé
- « anti-intrusion » comme un ensemble d'éléments anti-intrusion (intrusion et ouverture) y compris le système informatique associé

1.7.2.1.1 Condition d'exécution

Il est considéré 2 phases successives :

- la réalisation d'une ou des sous-prestations
- la réception d'une ou des sous-prestations

1.7.2.1.2 Les attendus de la phase réalisation

Au démarrage :

- Un plan d'implémentation et de câblage
- Le tableau des ouvrants dans le cas du contrôle des accès
- Un planning d'exécution des travaux- Un annuaire de contact identifié

Réunion et suivi :

- Une réunion de lancement en présentiel avec les parties prenantes des représentants du pouvoir adjudicateur et du bénéficiaire afin d'organiser le chantier
- Des visites de suivi de chantier régulières et transmission d'un reporting au maximum tous les 10 jours ouvrés de l'avancement des travaux
- La participation aux réunions techniques (en visio ou présentiel)

La réalisation inclut à minima :

- L'installation et le paramétrage des logiciels sur les serveurs et postes clients pour toutes les sous prestations
- La pose, le raccordement, le réglage et le paramétrage de tous les équipements pour toutes les sous prestations. La pose du câblage au mètre linéaire fait l'objet d'une ligne spécifique dans le BPU.

Pour les serrureries, se reporter au chapitre « FOURNITURE ET POSE DES SERRURERIES » du CCTP.

- La cérémonie des clés pour la sous-prestation contrôle d'accès
- Le paramétrage éventuel de renvoi de flux entre site pour la sous-prestation vidéo protection
- La mise en service et essais de l'ensemble pour toutes les sous-prestations

- La Mise en service et essais de la sauvegarde et de la restauration du système et plan de reprise pour les sous-prestations de vidéoprotection, contrôle d'accès et détection d'intrusion

Toutes autres actions ou tâches nécessaires à la mise en œuvre sont de la responsabilité du titulaire donc implicitement inclus dans le socle.

L'intégration se fera selon les règles établies dans le chapitre idoine du CCTP.

1.7.2.1.3 les attendus de la phase de réception

Les différentes étapes de cette phase et les livrables associés sont détaillés dans le chapitre « RÉCEPTION » de ce présent CCTP.

La prestation doit prévoir toutes les actions nécessaires à la bonne réalisation des différentes étapes de la réception de la solution ce qui inclut notamment :

- La réalisation de la recette fonctionnelle
- La réalisation de la recette câblage réseau (cuivre et fibre)
- La réalisation de la recette câblage courant fort
- La vérification de conformité au CCTP
- La visite de vérification d'aptitude
- Le suivi des levées de réserves « VÉRIFICATION APTITUDE AU BON FONCTIONNEMENT » (VABF)
- Le suivi des levées de réserves « VÉRIFICATION SERVICE RÉGULIER » (VSR)
- La fourniture des livrables documentaires attendus pour toutes les sous prestations
- La réalisation des formations pour toutes les sous-prestations
- Les différents procès-verbaux (PV)

1.7.2.1.4 les livrables attendus pour une ou plusieurs sous-prestation

Les livrables attendus selon la nature des actions réalisées sont les suivants :

En phase de réalisation :

Nom du livrable	Délai de production (titulaire)
Reporting avancement réalisation	Reporting écrit hebdomadaire (mail ou compte rendu d'activité) avec mise à jour éventuelle du planning

En phase de réception :

Il s'agira d'émettre des procès-verbaux (PV) avec réserves ou sans.

périmètre	Nom du livrable	Délai de livraison (titulaire)	Délai de validation (bénéficiaire)
Contrôle d'accès	PV des tests fonctionnels CA	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels CA	Avant le démarrage de la VABF	20jours ouvrés après la livraison
Vidéoprotection	PV des tests fonctionnels VP	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels VP	Avant le démarrage de la VABF	20jours ouvrés après la livraison

Détection d'intrusion	PV des tests fonctionnels Intrusion	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels Intrusion	Avant le démarrage de la VABF	20jours ouvrés après la livraison
Interphonie/ Visiophonie	PV des tests fonctionnels Interphone/visiophone	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels interphone/visiophone	Avant le démarrage de la VABF	20jours ouvrés après la livraison
Tous les périmètres	Reporting avancement réception	Reporting écrit hebdomadaire (mail ou compte rendu d'activité)	-
	Dossier de recette câblage cuivre	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Dossier de recette câblage fibre	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Dossier de recette courant fort	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Attestation de conformité au CCTP	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison
	Support de formation	5 jours avant la	20jours ouvrés après la livraison
	éventuel	formation	
	Dossier des Ouvrages exécutés (avec fiche technique matériel)	15 jours ouvrés après la visite de réception	20jours ouvrés après la livraison
	Manuel d'administration	5 jours avant la formation	20jours ouvrés après la livraison
	Manuel d'exploitation	5 jours avant la formation	20jours ouvrés après la livraison
	Consigne de sécurité pour le bon usage de la solution	Au plus tard à la fin de la VABF	20jours ouvrés après la livraison

Vidéoprotection, contrôle d'accès et détection d'intrusion	Procédure de sauvegarde / restauration	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Procédure de reprise des activités du système	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	PV de vérification d'aptitude	A la fin de la VABF	20 jours ouvrés après la livraison

La visite de vérification d'aptitude est obligatoire pour la validation.

1.7.3 PRESTATION P2 DE FOURNITURE, INSTALLATION, RACCORDEMENT ET MISE EN SERVICE D'UN SYSTÈME DE VIDÉO PROTECTION, DE CONTRÔLE D'ACCÈS, DE DÉTECTION D'INTRUSION, D'INTERPHONIE / VISIOPHONIE (EXTENSION D'UN SYSTÈME EXISTANT)

Le titulaire devra se référer à chaque annexe correspondante pour les conditions techniques de réalisation. Un chantier pourra intégrer une ou plusieurs sous-prestations selon le besoin.

1.7.3.1 les sous prestations

SP2.1 Fourniture, installation, raccordement et mise en service d'une extension d'un système de vidéo protection existant,

SP2.2 Fourniture, installation, raccordement et mise en service d'une extension d'un système de contrôle d'accès existant,

SP2.3 Fourniture, installation, raccordement et mise en service d'une extension d'un système de détection d'intrusion existant,

SP2.4 Fourniture, installation, raccordement et mise en service d'une extension d'un système d'interphonie / visiophonie existant

Chaque sous-prestation est considérée comme un ensemble incluant toutes les actions et livrables (hors acquisition matérielle unitaire, licences et dépose d'un existant, formation et pose câblage) nécessaire à la livraison d'un système (solution opérationnelle).

La pose, le raccordement et le paramétrage des matériels et équipements informatiques existant et acquis font partie du socle.

La mise à jour de la documentation et les livrables font partie du socle.

Les différents tests et recette font partie du socle. La mise en service de l'extension fait partie du socle Le BPU mentionne des tranches considérant :

- « porte » comme un ensemble d'éléments permettant de la sécuriser à intégrer dans un système existant (par ex l'association de lecteurs de badge en entrée et possiblement en sortie, d'une serrure, d'une ventouse, d'un BG vert ou d'un bouton sortie, un possible asservissement à la centrale incendie ...)

Une sécurisation correspond à minima à un lecteur de badge de contrôle d'accès.

- « caméra » comme un ensemble d'élément vidéo à intégrer dans un système existant
- « anti-intrusion » comme un ensemble d'éléments anti-intrusion (intrusion et ouverture) à intégrer dans un système existant

1.7.3.1.1 Condition d'exécution

Il est considéré 2 phases successives :

- la réalisation d'une ou des sous-prestations
- la réception d'une ou des sous-prestations

1.7.3.1.2 Les attendus de la phase réalisation

Au démarrage :

- Un plan d'implémentation et de câblage
- Un planning d'exécution des travaux
- Un annuaire de contact identifié

Réunion et suivi :

- Des visites de suivi de chantier régulières et transmission d'un reporting au maximum tous les 10 jours ouvrés de l'avancement des travaux
- La participation aux réunions techniques (en visio ou présentiel)

La réalisation inclut à minima :

- L'installation et le paramétrage des logiciels sur les serveurs et postes clients pour toutes les sous prestations
 - La pose, le raccordement, le réglage et le paramétrage de tous les équipements pour toutes les sous prestations. La pose du câblage au mètre linéaire fait l'objet d'une ligne spécifique dans le BPU.
- Pour les serrureries, se reporter au chapitre « FOURNITURE ET POSE DES SERRURERIES » du CCTP.
- Le paramétrage éventuel complémentaire de renvoi de flux entre site pour la sous-prestation vidéo protection
 - La mise en service et essais des extensions et vérification non régression du fonctionnement de l'ensemble pour toutes les sous-prestations
 - La vérification de la sauvegarde, la restauration du système et le plan de reprise pour les sous prestations de vidéoprotection, contrôle d'accès et détection d'intrusion suite aux ajouts devront comprendre :
 - la vérification de la prise en compte des extensions et ajouts réalisés dans les mécanismes de sauvegarde existants ;
 - le contrôle des paramètres de sauvegarde (périmètre, périodicité, supports, rétention) ;
 - la réalisation d'au moins un test de restauration, partiel ou complet, sur un environnement défini avec le maître d'ouvrage ;
 - la démonstration du bon fonctionnement du système après restauration.

Les modalités de sauvegarde et de restauration, ainsi que les résultats des tests, devront être documentés et intégrés aux livrables de recette et au DOE.

Toutes autres actions ou tâches nécessaires à la mise en œuvre sont de la responsabilité du titulaire donc implicitement inclus dans le socle.

L'intégration se fera selon les règles établies dans le chapitre idoine du CCTP.

1.7.3.1.3 les attendus de la phase de réception

Les différentes étapes de cette phase et les livrables associés sont détaillés dans le chapitre « RÉCEPTION » de ce présent CCTP.

La prestation doit prévoir toutes les actions nécessaires à la bonne réalisation des différentes étapes de la réception de la solution ce qui inclut notamment :

- La réalisation de la recette fonctionnelle
- La réalisation de la recette câblage réseau (cuivre et fibre)
- La réalisation de la recette câblage courant fort
- La vérification de conformité au CCTP
- La visite de vérification d'aptitude

- Le suivi des levées de réserves « VÉRIFICATION APTITUDE AU BON FONCTIONNEMENT » (VABF)
- Le suivi des levées de réserves « VÉRIFICATION SERVICE RÉGULIER » (VSR)
- La fourniture des livrables documentaires MIS A JOUR attendus pour toutes les sous prestations- La réalisation des formations éventuelles pour toutes les sous-prestations
- Les différents procès-verbaux (PV)

1.7.3.1.4 les livrables attendus pour une ou plusieurs sous-prestation

Les livrables attendus selon la nature des actions réalisées sont les suivants :

En phase de réalisation :

Nom du livrable	Délai de production (titulaire)
Reporting avancement réalisation	Reporting écrit hebdomadaire (mail ou compte rendu d'activité) avec mise à jour éventuelle du planning

En phase de réception :

Il s'agira d'émettre des procès-verbaux (PV) avec réserves ou sans.

périmètre	Nom du livrable	Délai de livraison (titulaire)	Délai de validation (bénéficiaire)
Contrôle d'accès	PV des tests fonctionnels CA	À la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels CA	Avant le démarrage de la VABF	20jours ouvrés après la livraison
Vidéoprotection	PV des tests fonctionnels VP	À la fin de la VABF	20jours ouvrés après la livraison
	Cahier des tests fonctionnels VP	Avant le démarrage de la VABF	20jours ouvrés après la livraison

Détection d'intrusion	PV des tests fonctionnels Intrusion	À la fin de la VABF	20 jours ouvrés après la livraison
	Cahier des tests fonctionnels Intrusion	Avant le démarrage de la VABF	20 jours ouvrés après la livraison

Interphonie/ Visiophonie	PV des tests fonctionnels Interphone/ visiophone	À la fin de la VABF	20 jours ouvrés après la livraison
	Cahier des tests fonctionnels interphone/ visiophone	Avant le démarrage de la VABF	20 jours ouvrés après la livraison
Tous les périmètres	Reporting avancement réception	Reporting écrit hebdomadaire (mail ou compte rendu d'activité)	-
	Dossier de recette câblage cuivre	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Dossier de recette câblage fibre	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Dossier de recette courant fort	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Attestation de conformité au CCTP	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Support de formation éventuel	5 jours avant la formation	20 jours ouvrés après la livraison
	Dossier des Ouvrages exécutés (avec fiche technique matériel)	15 jours ouvrés après la visite de réception	20 jours ouvrés après la livraison
	Manuel d'administration	5 jours avant la formation	20 jours ouvrés après la livraison
	Manuel d'exploitation	5 jours avant la formation	20 jours ouvrés après la livraison
	Consigne de sécurité pour le bon usage de la solution	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison

Vidéoprotection, contrôle d'accès et détection d'intrusion	Procédure de sauvegarde / restauration	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	Procédure de reprise des activités du système	Au plus tard à la fin de la VABF	20 jours ouvrés après la livraison
	PV de vérification d'aptitude	A la fin de la VABF	20 jours ouvrés après la livraison

La visite de validation d'aptitude est obligatoire pour la validation.

1.7.4 PRESTATION P3 DE DÉMONTAGE/DÉPOSE

1.7.4.1 Démontage/dépose

Le démontage comprend la dépose des installations devenues inutiles (caméras, écrans, enregistreur, détecteurs, lecteurs de badges, fixations, réglettes de câblage, câbles, boîtes de distribution, prises, serrures, etc.), supports de câbles inclus (tubes, goulottes, plinthes, moulures, etc.). Ce démontage sera effectué soigneusement. Tous les câbles colliers, attaches, ferrures seront enlevés et les trous rebouchés. Les anciennes prises encastrées seront obturées par des caches appropriés.

Le maintien de certains câbles dont le démontage entraînerait des dégradations trop importantes du point de vue esthétique (éclats de peinture, etc.) est soumis à l'accord du bénéficiaire. Ces câbles seraient alors laissés sur place et coupés à ras, de manière à rendre leur inutilité évidente et à faciliter leur retrait lors de travaux futurs.

Le bénéficiaire se réserve le droit de conserver tout ou partie du matériel démonté.

Cette prestation sera définie avec le prestataire lors de la visite de site.

1.7.4.2 Stockage

Un local fermant à clé sera mis à disposition du titulaire par le bénéficiaire. Son emplacement sera défini lors de la visite de site en accord avec la DSI. Ce local permettra d'entreposer le matériel en attente d'installation ainsi que tout élément démonté.

1.7.4.3 Recyclage

Le titulaire prendra à sa charge l'enlèvement et le recyclage de tout matériel démonté. Le recyclage devra être réalisé auprès des organismes de collecte agréés.

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 au bénéficiaire qui se chargera de les détruire. Aucune donnée ne peut être dupliquée sur tout support hors du site conformément aux recommandations SSI.

1.7.5 PRESTATION P4 DE FORMATION/TRANSFERT DE COMPETENCES

La prestation de formation a pour objet le transfert de compétences nécessaire à l'exploitation, au bénéficiaire et au maintien en conditions opérationnelles des systèmes de sûreté électronique mis en œuvre.

Les formations dispensées devront être nécessaires et suffisantes pour permettre aux personnels désignés par le bénéficiaire d'exercer leurs missions en autonomie, dans le respect des fonctionnalités et des règles d'exploitation des solutions déployées.

Les formations seront assurées par des formateurs spécialisés, dûment habilités par le ou les fournisseurs des solutions intégrées, et disposant d'une attestation ou certification éditeur en lien avec les systèmes déployés.

Les formations se dérouleront sur site, selon des modalités validées avec le bénéficiaire.

Les supports de formation seront fournis en langue française, en version papier et en version électronique, dans des formats lisibles à l'aide de logiciels libres.

Le titulaire proposera, pour validation par le bénéficiaire, le contenu, la durée et le nombre de sessions, en fonction:

- des profils des participants ;
- du périmètre fonctionnel réellement mis en œuvre ;
- du nombre de participants par catégorie (administrateurs, exploitants).

À l'issue des formations, le titulaire fournira :

- les supports pédagogiques utilisés ;
- une attestation de réalisation des formations ;
- la liste des participants formés.

La réalisation complète des formations conditionne la validation de la prestation P4.

1.7.5.1 Formation des Administrateurs

La formation des administrateurs a pour objectif de permettre une maîtrise complète des systèmes de sûreté électronique mis en œuvre, tant sur les aspects de configuration que d'administration et de supervision.

Elle couvre notamment :

- l'administration des applications et des plateformes ;
- la gestion des comptes et des habilitations ;
- la gestion des paramètres fonctionnels et temporels ;
- la configuration des scénarios et règles de fonctionnement ;
- la gestion des sauvegardes et des restaurations ;
- l'administration des données, images et journaux ;
- les opérations nécessaires au maintien en conditions opérationnelles.

La formation doit permettre aux administrateurs d'assurer l'exploitation avancée, l'évolution et le support de premier niveau des systèmes.

1.7.5.2 Formation des Gestionnaires de badges

La formation des gestionnaires de badges vise à permettre l'exploitation autonome des fonctions liées à l'enrôlement et à la gestion des identités et des supports d'accès.

Elle comprend notamment :

- la gestion des profils et droits d'accès ;
- l'émission, la modification et la suppression des badges ;
- la gestion des calendriers et plages horaires ;
- les opérations courantes liées à l'accueil et aux badges temporaires.

La formation devra permettre une gestion quotidienne sécurisée et conforme aux règles définies par le bénéficiaire.

1.7.5.3 Formation des Exploitants/Opérateurs

La formation des exploitants (opérateurs) a pour objectif de permettre une utilisation optimale et sécurisée des systèmes de sûreté électronique dans le cadre de l'exploitation quotidienne.

Elle couvre notamment :

- la prise en main des postes et équipements d'exploitation ;
- l'utilisation des interfaces logicielles ;
- l'exploitation des systèmes de vidéoprotection, contrôle d'accès, détection d'intrusion et visiophonie ;
- la gestion des événements, alarmes et incidents ;
- les opérations courantes liées à l'accueil et aux visiteurs.

La formation devra permettre aux exploitants d'assurer leurs missions dans le respect des procédures opérationnelles et des règles de sécurité définies.

1.7.6 PRESTATIONS DE MAINTENANCE ET D'EXPLOITATION DES SYSTEMES DE SURETE

1.7.6.1 Objet des prestations

Le présent chapitre a pour objet de définir les prestations de maintenance et d'exploitation applicables aux systèmes de sûreté électronique mis en œuvre dans le cadre du présent marché zonal, incluant notamment :

- Les systèmes de vidéoprotection / vidéosurveillance ;
- Les systèmes d'anti-intrusion, y compris les dispositifs raccordés à une télésurveillance ;
- Les systèmes de contrôle d'accès et de gestion des habilitations.

Les prestations de maintenance ont pour finalité de garantir, sur toute la durée du marché, la disponibilité opérationnelle, la continuité de service, la pérennité des équipements et la maîtrise de l'exploitation des systèmes déployés.

1.7.6.2 Périmètre général de la maintenance

La maintenance couvre l'ensemble des équipements, logiciels, infrastructures et services associés aux systèmes de sûreté, incluant notamment :

- Les équipements actifs (caméras, détecteurs, lecteurs, centrales, serveurs, enregistreurs, équipements réseau dédiés) ;
- Les équipements passifs liés au fonctionnement des systèmes (alimentations, coffrets, protections) ;
- Les logiciels de supervision, d'administration et d'exploitation ;
- Les liaisons et interfaces nécessaires au bon fonctionnement des systèmes, dans le respect des périmètres de responsabilité définis.

La maintenance s'applique aux sites existants et aux sites intégrés progressivement dans le cadre du marché zonal.

1.7.6.3 Typologie des prestations de maintenance

Les prestations attendues sont structurées selon les niveaux suivants :

1.7.6.3.1 Maintenance préventive

La maintenance préventive a pour objectif de prévenir les défaillances et de maintenir les équipements dans un état de fonctionnement optimal.

Elle comprend notamment :

- Les visites périodiques planifiées ;
- Les vérifications fonctionnelles complètes des systèmes ;
- Le nettoyage des équipements (optique des caméras, lecteurs, capteurs) ;
- Les tests de fonctionnement et de communication ;
- Les vérifications d'alimentation et de continuité électrique ;
- Les mises à jour mineures et correctives des logiciels et firmwares, après validation du pouvoir adjudicateur.

Les fréquences minimales d'intervention devront être précisées par le titulaire dans son offre.

1.7.6.3.2 Maintenance corrective

La maintenance corrective a pour objet le rétablissement du service en cas de dysfonctionnement ou de panne.

Elle comprend notamment :

- Le diagnostic des incidents ;
- Les interventions de dépannage sur site ou à distance ;
- Le remplacement ou la réparation des équipements défectueux ;
- Les opérations de reparamétrage et de remise en configuration ;
- Les tests de remise en service.

Les délais d'intervention et de rétablissement devront être compatibles avec la criticité des sites et des systèmes concernés.

1.7.6.3 Maintenance évolutive et assistance à l'exploitation

La maintenance évolutive et l'assistance à l'exploitation visent à accompagner le pouvoir adjudicateur dans la durée. Elle comprend notamment :

- L'assistance technique avancée aux exploitants ;
- L'accompagnement à l'évolution des paramétrages ;
- L'assistance post-incident ou post-événement de sûreté ;
- L'appui à l'exploitation opérationnelle (extractions vidéo, journaux d'événements, analyses techniques) ;
- Le support technique dans le cadre de procédures administratives ou judiciaires, dans le respect de la réglementation en vigueur.

1.7.6.4 Organisation et modalités d'intervention

Le titulaire devra mettre en place une organisation adaptée à un marché zonal multisites, incluant :

- Un point de contact identifié pour la maintenance ;
- Une capacité d'intervention sur l'ensemble du périmètre géographique concerné ;
- Une gestion structurée des demandes d'intervention (outil de ticketing ou GMAO).

Toute intervention devra donner lieu à un compte rendu détaillé transmis au pouvoir adjudicateur.

1.7.6.5 Niveaux de service et engagements

Le titulaire s'engage à respecter des niveaux de service (SLA) définis dans le cadre du marché, portant notamment sur :

- Les délais de prise en charge ;
- Les délais d'intervention ;
- Les délais de rétablissement du service.

Les engagements de service devront être compatibles avec la sensibilité des sites et la criticité des systèmes de sûreté.

1.7.6.6 Prestations de télésurveillance (optionnel)

Lorsque les systèmes d'anti-intrusion sont raccordés à une prestation de télésurveillance, le titulaire devra garantir :

- La compatibilité technique des équipements avec les centres de télésurveillance ;
- La continuité des transmissions ;
- La gestion des alarmes et événements selon les consignes définies par le pouvoir adjudicateur ;
- La traçabilité des événements et interventions.

Les prestations de télésurveillance devront être conformes à la réglementation en vigueur.

1.7.6.7 Traçabilité, reporting et documentation

Le titulaire devra assurer une traçabilité complète des opérations de maintenance, incluant :

- L'historique des interventions ;
- Les incidents et actions correctives ;
- Les équipements remplacés ;
- Les mises à jour réalisées.

Des rapports périodiques de maintenance devront être transmis selon une périodicité définie au marché.

1.7.6.8 indépendance technologique et pérennité

Les prestations de maintenance devront être assurées dans le respect des principes suivants :

- Absence de dépendance exclusive à un constructeur ou à une technologie propriétaire ;
- Maintenabilité des solutions sur la durée du marché ;
- Possibilité d'évolution et de réversibilité des systèmes.

1.7.6.9 Modalités financières

Les prestations de maintenance feront l'objet :

- D'un chiffrage distinct dans les pièces financières du marché ;
- De forfaits et/ou de prix unitaires clairement identifiés ;
- D'une activation progressive par site ou par périmètre, selon les besoins du pouvoir adjudicateur.

Les seuils indiqués dans le BPU constituent des seuils de référence destinés à l'analyse financière des offres. Le périmètre réel de maintenance pourra être ajusté par émission de bon de commande, notamment par activation de tranches complémentaires

1.7.6.10 Modalités de mise en œuvre dans le cadre d'un marché à bons de commande

Les prestations de maintenance définies au présent chapitre sont exécutées exclusivement sur émission de bons de commande, conformément aux dispositions du marché.

Aucune prestation de maintenance ne pourra être considérée comme acquise sans bon de commande exprès du pouvoir adjudicateur.

Les bons de commande pourront porter notamment sur :

- L'activation de la maintenance d'un site existant ;
- L'intégration d'un nouveau site dans le périmètre de maintenance ;
- La souscription ou l'arrêt d'une prestation de maintenance ;
- Des interventions ponctuelles de maintenance corrective ou évolutive.

1.7.6.11 Activation progressive et périmètre variable

Le périmètre de maintenance est évolutif sur la durée du marché zonal.

Le pouvoir adjudicateur se réserve la possibilité :

- D'activer la maintenance par site ou par groupe de sites ;
- De différencier les niveaux de maintenance selon la criticité ;
- D'adapter les prestations aux besoins réels constatés.

5.12 Absence d'exclusivité et continuité de service

La passation de bons de commande de maintenance n'emporte aucune exclusivité automatique sur l'ensemble des systèmes existants.

Les prestations devront garantir la continuité de service, y compris lors de l'intégration progressive de nouveaux sites ou systèmes hétérogènes.

1.7.6.13 Cohérence avec les prestations d'installation, de mise en service et de maintenance

Les prestations de maintenance pourront être activées :

- À l'issue des phases d'exécution et de mise en service ;
- Après réception partielle ou totale des installations ;
- Indépendamment des autres sites du marché zonal.

2 LES EXIGENCES ET SPÉCIFICITÉS DES SYSTÈMES

2.1 INFRASTRUCTURE RÉSEAU

ATTENTION !

Elle sera réalisée conformément aux principes décrits dans l'annexe à ce CCTP dénommée
ANNEXE 1 - CCTP SURETE PRINCIPES CABLAGE EQUIPEMENTS RACCORDEMENT

Rappel : 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.

Rappel : Les travaux de câblage seront exécutés conformément aux spécifications générales relatives aux systèmes de câblage pour réseaux de communication du Ministère de l'Intérieur (M.I.).

2.1.1 LA DORSALE OPTIQUE

Le Ministère de l'Intérieur fournit les caractéristiques des liens optiques nécessaires à l'interconnexion des éléments actifs du réseau de sûreté.

2.1.2 LE CAPILLAIRE CUIVRE

Tous les périphériques de type « Ethernet/IP » (serveurs, stations, caméras, UTL, etc.) proposés dans la solution seront raccordés sur les répartiteurs désignés par l'administration (et dans la plupart des cas, le plus proche) par un lien « Ethernet », ou fibre optique multimode à la charge du titulaire en respectant les règles de l'art.

Les cordons ou jarretières de brassage et de raccordement sont à fournir par le titulaire.

2.1.3 LES BAIES

Le titulaire fournira si nécessaire en fonction de l'existant la ou les baies conformes à l'annexe.

Il devra s'assurer que l'ensemble des baies soit équipé d'un onduleur tel que décrit dans l'annexe.

2.1.4 LES ÉLÉMENTS ACTIFS

Le titulaire proposera le nombre de commutateurs réseau à mettre en œuvre. Le Ministère de l'Intérieur les fournira ainsi que le plan d'adressage IP.

Le titulaire complètera le document de matrice des flux nécessaires à la mise en œuvre des installations type pare-feu.

2.1.5 CÂBLAGE SPÉCIFIQUE SÛRETÉ BATIMENTAIRE

Un besoin spécifique au raccordement des éléments de sûreté est à prévoir dans l'offre.

Les liaisons cuivre et les liaisons optiques répondront aux spécificités générales de ce présent CCTP.

Les prises RJ 45 devront être câblées dans les baies sur des bandeaux spécifiques identifiés sûreté. Le positionnement des extrémités des liaisons côté périphérique (UTL, lecteur de badges, caméras, stations de supervision et de gestion) sera réalisé conformément aux plans fournis. Les différents types de câbles sont décrits dans l'annexe 1.

Il est rappelé que les liaisons cuivre 4 paires utiliseront des câbles 4 paires écrantés F/FTP 100 □ de catégorie 6A, avec croix de séparation des paires, compatibles avec la norme POE étendu 24W (classe Ea norme ISO/IEC 11801) Les liaisons optiques pourront être monomode ou multimode, connectiques SC ou LC, version UPC ou APC, selon les besoins

2.1.5.1 UTL contrôle d'accès

Pour les UTL (ou concentrateur selon la solution retenue) il est demandé une liaison Ethernet entre l'UTL et le bandeau RJ 45 dédié sûreté.

L'interconnexion entre les UTL et les bandeaux se fera sans point de coupure, ou à défaut en cas d'impossibilité l'extrémité de la liaison côté UTL se terminera sur une prise RJ45 en saillie à proximité immédiate de l'UTL.

(Soumis à l'accord du Ministère)

Les UTL devront être positionnées dans les locaux répartiteurs ou dans des pièces sécurisées pour interdire l'accès à toutes personnes non autorisées.

2.1.5.2 Lecteurs de badges

Cette prestation sera réalisée par le titulaire du contrôle d'accès en respectant les spécifications techniques des lecteurs de badges qu'il aura choisi.

2.1.5.3 Caméras

Pour les besoins de raccordement des caméras de vidéoprotection il est demandé une liaison Ethernet ou optique si nécessaire entre la caméra et le bandeau RJ 45 dédié sûreté.

L'extrémité de la liaison côté caméra se fera sans point de coupure ou à défaut sur une prise RJ45 en saillie à proximité immédiate des caméras avec accord du Ministère (attention au positionnement pour les caméras extérieures car il sera préférable de laisser le point d'accès à l'intérieur du bâtiment).

L'installateur des caméras se chargera de la perforation du mur pour le raccordement.

2.1.5.4 Station de supervision et de gestion

Pour les besoins de raccordement des stations de supervision du contrôle d'accès et de la vidéoprotection il est demandé une liaison Ethernet banalisée entre la station caméra et le bandeau RJ45 dédié qui se trouve dans la baie sûreté.

L'extrémité de la liaison côté Station de supervision se terminera sur une prise RJ45 en saillie à proximité immédiate de la Station.

2.1.5.5 Cordons de brassage

Les cordons de brassage et de raccordement sont à fournir par le titulaire

Le titulaire proposera la fourniture de cordons 4 paires F/FTP 100 □ de catégorie 6A compatibles avec la norme POE étendu 24W (classe Ea norme ISO/IEC 11801)

Afin de pouvoir identifier facilement les différents types de périphériques, les cordons fournis devront répondre au code des couleurs suivants :

Périphérique	Couleur
Vidéo-protection	Violet
Contrôle d'accès (UTL, etc.)	Orange
Visiophonie	Bleu
Alarme	Vert
Divers	Gris

2.2 SYSTÈME DE CONTRÔLE D'ACCÈS

ATTENTION !

Les prestations seront réalisées conformément aux principes décrits dans l'annexe à ce CCTP dénommée :

ANNEXE 2 - CCTP SURETE PRINCIPES CONTROLE ACCES

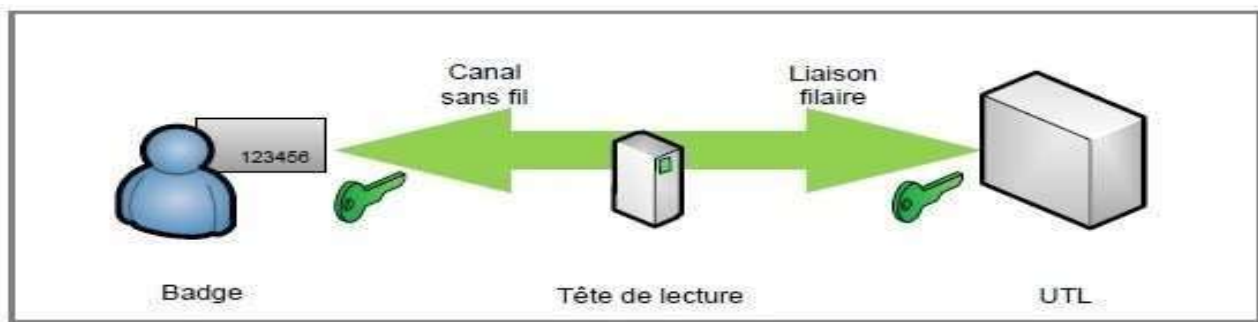
2.2.1 COMPATIBILITÉ

Le système installé doit être compatible avec la carte agent du ministère de l'intérieur.

2.2.2 GÉNÉRALITÉS

Le système de contrôle d'accès se reposera sur l'architecture N°1 décrite dans le guide de l'ANSSI : tête de lecture transparente, authentification de bout en bout.

La solution sera de type client / serveur et sera pourvu d'une double alimentation. (1 directe 220v et 1 secourue par un onduleur à fournir pour une autonomie de 20mn)



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

Le système de contrôle d'accès sécurisé sera géré à partir d'un poste dédié sûreté.

L'ensemble sera bâti autour d'une solution IP.

En supplément des recommandations de l'ANSSI, les UTLs seront impérativement installées dans les locaux sécurisés sauf avis contraire de l'administration.

Les lecteurs seront en version Mifare DesFire Ev2, compatibles EV1 et devront accepter les badges agent du ministère de l'Intérieur (informations techniques référencées dans l'annexe 2)

2.2.3 SOLUTION DE CONTRÔLE D'ACCÈS CERTIFIÉE ANSSI

Seuls les produits de fabricants bénéficiant au minimum d'un certificat de sécurité de premier niveau (CSPN) de l'ANSSI, en cours de validité ou de renouvellement sont acceptés pour les installations de systèmes de contrôle d'accès des sites du ministère de l'Intérieur. Il appartient à l'installateur de vérifier que le fabricant de la solution de contrôle d'accès est certifié par l'ANSSI.

NB : Le Certificat de Sécurité de Premier Niveau a une validité de 3 ans.

Il sera admis donc que du matériel, composant ou solution puisse être en cours de renouvellement de certification. Dans ce cadre, une preuve écrite d'une démarche de renouvellement de certification en cours sera nécessaire.

2.2.4 FOURNITURE ET POSE DES SERRURIES

La fourniture et la pose physique d'éléments de serrurerie dans des menuiseries existantes intérieures ou extérieures font partie du présent CCTP, elles devront être réalisées sans altération de l'intégrité mécanique des menuiseries.

La pose physique d'éléments de serrurerie dans des menuiseries neuves devront être réalisées par le fournisseur des menuiseries neuves afin d'en préserver l'intégrité.

La fourniture d'éléments de serrurerie dans des menuiseries neuves est possible par ce marché cependant l'acquisition doit se faire en accord avec le menuisier (dimension, type de serrure Xpoints attendus selon la sécurité de la porte etc.).

L'intégration dans la solution de gestion est à la charge du titulaire. Se référer aux prestations P1 et P2.

2.2.5 OBSTACLES MÉCANIQUES

Les obstacles mécaniques (Tourniquets, barrières etc.) sont exclus du marché.

2.2.6 MAQUETTE ET CÉRÉMONIE DES CLÉS (USINE)

Avant le déploiement en production, le déploiement de la solution prévue sur une plateforme maquette est fortement recommandée. Celle-ci sera dans la mesure du possible représentative de l'environnement de production (avec éléments de sécurité - filtrage). Le périmètre de la maquette et les résultats des tests seront à communiquer à l'Administration.

Le titulaire devra également tester en usine la cérémonie des clés (avec des clés de test) afin de fiabiliser cette étape clé de mise en service.

2.3 SYSTÈME DE DÉTECTION INTRUSION

ATTENTION !

La prestation sera réalisée conformément aux principes décrits dans l'annexe à ce CCTP dénommée
ANNEXE 3 - CCTP SURETE PRINCIPES DETECTION INTRUSION

2.4 SYSTÈME DE VIDÉO-PROTECTION

ATTENTION !

La prestation sera réalisée conformément aux principes décrits dans l'annexe à ce CCTP dénommée
ANNEXE 4 - CCTP SURETE PRINCIPES VIDEO PROTECTION

Tous les équipements installés seront de technologie IP.

Les caméras seront raccordées par câbles réseau Cat 6A (cf supra), et alimentées et secourues en POE à partir du ou des commutateurs.

2.5 CAS DE SOLUTION UNIFIÉE VIDEOPROTECTION ET CONTRÔLE D'ACCÈS

L'objectif de la solution est d'une part de fédérer une application traditionnelle de contrôle d'accès ou de vidéo-protection et, d'autre part, de superviser le système en proposant sur une interface unifiée la gestion des accès, alarmes et vidéo.

Cette solution peut être constituée d'un superviseur client de deux systèmes disjoints : contrôle d'accès et système vidéo.

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.

La référence d'horodatage sera donnée par le serveur de temps.

3 LES EXIGENCES DOCUMENTAIRES, D'ADMINISTRATION ET D'EXPLOITATION

3.1 DOCUMENTATIONS

Les documentations sont livrées en français, en version numérique (sous forme de fichier électronique lisibles à partir de logiciels libres.), et en version papier lorsque cela est mentionné. Ces documents devront revêtir le timbre « DIFFUSION RESTREINTE ».

3.1.1 DOCUMENTATION TECHNIQUE

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

- Le mémoire technique de la solution (si étude réalisée)
- Les documentations techniques en français des matériels installés, - Les documentations personnalisées d'exploitation de la solution déployée - Le Dossier des Ouvrages Exécutés (D.O.E.) comprenant :
 - L'emplacement de tous les équipements installés (caméras, détecteurs, UTL, postes clients, ...) sur des plans mis à jour au format dwg et pdf,
 - Un inventaire de tous les équipements posés (modèle, référence produit, quantité, niveau firmware, date de début de garantie, durée de garantie ...)
 - Fiches techniques des matériels
 - Prises de vues de référence des caméras,
 - Le cheminement des câbles posés (courant fort et faible),
 - Les adresses IP de chaque équipement
 - Le tableau des ouvrants pour le contrôle d'accès
 - Le synoptique des solutions déployées

Une trame du DOE sera fournie par l'administration, le titulaire se chargera de renseigner les champs concernés et de fournir les pièces demandées.

3.1.2 DOCUMENTATION D'ADMINISTRATION ET D'EXPLOITATION

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

- Un manuel d'administration système et des applications,
- un manuel utilisateur 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.

3.1.3 SAUVEGARDE ET RESTAURATION

Le titulaire devra mettre en place une sauvegarde complète hebdomadaire des systèmes de contrôle d'accès et de vidéo protection mis en place, l'objectif étant de pouvoir repartir de ces sauvegardes en cas de panne matérielle ou de perte de configuration ou de paramétrage.

La durée de rétention sera de 30 jours en rotation.

Pour cela le titulaire devra également s'appuyer sur les préconisations de l'éditeur.

Les sauvegardes récurrentes devront se faire automatiquement au travers d'un paramétrage des outils de sauvegarde intégrés à la solution ou au travers de scripts fournis par l'éditeur ou le titulaire le cas échéant

Concernant la vidéo protection, les sauvegardes ne couvrent pas les enregistrements vidéo La solution de sauvegarde devra contenir à minima :

- Une sauvegarde des bases de données et paramétrages applicatifs
- Une sauvegarde de l'état du système (base de registre, répertoire windows) avec les fichiers de configuration de la solution (liste fournis par l'éditeur)

Les sauvegardes se feront sur un disque NAS fourni par le titulaire raccordé sur les switchs sûreté du ministère de l'Intérieur.

Chaque système aura son propre disque NAS

Le titulaire devra mettre à disposition la documentation décrivant la procédure de sauvegarde mise en place ainsi que la procédure de restauration associée

Cette documentation devra également décrire la procédure à suivre pour lancer une sauvegarde à la demande nécessaire notamment en cas d'opération de maintenance ou de mise à jour du système

3.2 LA RÉCEPTION (VABF ET VSR)

La phase de réception vise à vérifier que la livraison est conforme. Elle est composée d'une vérification d'aptitude au bon fonctionnement (VABF) et d'une vérification en service régulier (VSR).

3.2.1 VABF

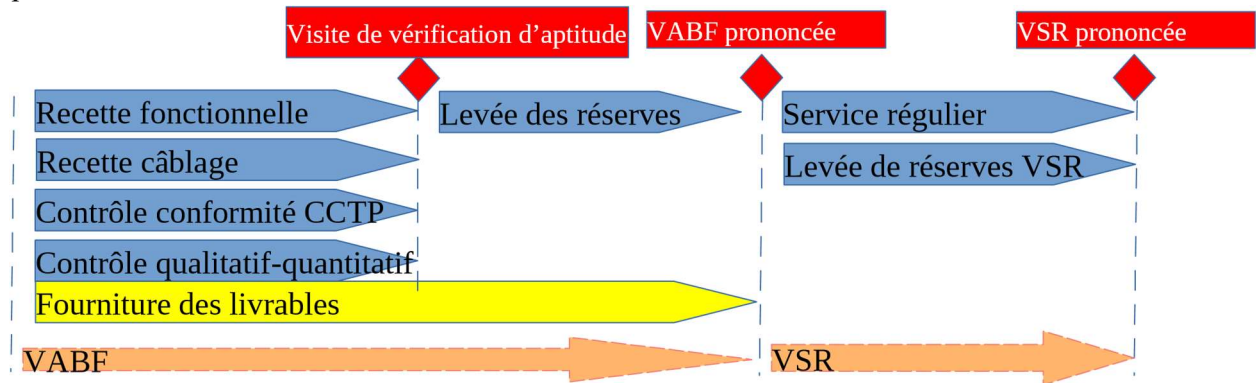
La vérification d'aptitude et de bon fonctionnement (VABF) porte sur les conditions suivantes :

- La réalisation avec succès de la recette fonctionnelle
- La conformité du quantitatif et qualitatif des équipements installés au regard de l'offre
- Le respect des spécifications du CCTP
- La livraison de la documentation attendue (DOE, document d'exploitabilité etc)
- La livraison des attestations attendues
- La livraison des dossiers recettes câblage attendues - La réalisation des formations attendues etc.

La VABF se termine lorsque toutes les conditions ci-dessus sont respectées.

Une visite de vérification d'aptitude sera organisée pour évaluer les réserves éventuelles.

La réception se déroulera selon le schéma suivant :



3.2.1.1 Les recettes

Elle est préalable à la vérification d'aptitude au bon fonctionnement.

3.2.1.1.1 Recette fonctionnelle

Chaque système : contrôle d'accès, intrusion, système vidéo, visiophonie, postes de travail devra faire l'objet d'une batterie de tests fonctionnels spécifiques permettant de garantir le bon fonctionnement des équipements livrés.

Ces tests seront réalisés par le titulaire en toute autonomie sauf pour les tests qui auraient un impact organisationnel sur les services en local (test centrale incendie, test de coupure électrique) et nécessiteraient une coordination en local auquel cas le titulaire se rapprocherait du représentant du ministère de l'Intérieur pour organiser et planifier la réalisation de ces tests spécifiques.

La réalisation de cette recette est une condition pour planifier la visite de vérification d'aptitude.

Le dossier de recette fonctionnelle est fourni par l'administration et liste les tests à réaliser à minima pour chaque système

A la charge du titulaire :

- D'ajouter d'éventuels tests complémentaires dans les dossiers de tests qu'il jugerait nécessaires à la bonne vérification du système
- De consigner le résultat de chaque test réalisé dans le PV de tests fonctionnels
- De procéder à la correction rapide des dysfonctionnements constatés
- De transmettre à l'administration les PV de tests fonctionnels

La date de livraison du PV de tests fonctionnels sera consignée dans le procès verbal de vérification d'aptitude et les PV de tests seront mis en annexes.

Le contrôle devra notamment 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.

3.2.1.1.2 Recette câblage

Elle couvre le courant fort et faible et l'infrastructure.

La recette du câblage se compose d'un contrôle d'inventaire, d'un contrôle visuel, d'une recette des liaisons cuivre et optique ainsi qu'une recette du courant fort.

La recette technique est l'opération qui doit permettre de garantir à l'Administration que l'installation est conforme :

- Au C.C.T.P.,
- 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.

◦ Recette des liaisons cuivre

Cette recette comprendra notamment, pour chaque liaison permanente (permanent link), la mesure des paramètres définis dans la norme ISO/IEC 11801 2^e édition 1^{er} amendement en classe Ea PL2 + PoE . La recette des liaisons cuivre 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.

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 dépairage,
- De la résistance en boucle,
- De l'exactitude de son identification par rapport aux plans d'installation.

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.

◦ Recette des liaisons optiques

Cette recette comprendra notamment, pour chaque liaison permanente (permanent link), la mesure des paramètres définis dans la norme ISO/IEC 11801 2^e édition 1^{er} amendement en classe Ea PL2 + PoE . La recette des liaisons optiques 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.

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.

- Recette du courant fort

Un contrôle fonctionnel permettra de vérifier :

- 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.

3.2.1.1.3 Recette de Conformité au CCTP

Les prestations réalisées pour les différents domaines, câblage, contrôle d'accès, intrusion, système vidéo, visiophonie, postes de travail devront être conformes au CCTP

Tout écart devra être remonté par le titulaire et faire l'objet d'une validation de la part du représentant du ministère de l'Intérieur

Une attestation de conformité sera fournie par le titulaire avec les dérogations éventuelles qui auraient pu être accordées.

Un contrôle échantillonné sera réalisé par le représentant du ministère de l'Intérieur lors de la visite de vérification d'aptitude.

3.2.1.1.4 Le contrôle quantitatif et qualitatif

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

Le titulaire fournit un inventaire des équipements installés (modèle, quantité)

Cet inventaire servira de support lors de la visite de réception et constitue un livrable attendu.

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.

Un contrôle visuel complètera et se portera sur la qualité générale de la prestation. Il sera vérifié notamment :

- Le respect des contraintes d'environnement,
- La mise en œuvre des câbles (y compris fixation et connexion) et leur cheminement,
- 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.

3.2.2 VISITE DE VALIDATION D'APTITUDE

Cette visite sera organisée par le représentant du ministère de l'Intérieur en présence du titulaire et du client final.

Pendant cette visite, des tests et des vérifications seront réalisés afin de contrôler le bon fonctionnement de la solution et sa conformité au CCTP et à l'offre initiale.

Un PV de validation d'aptitude sera dressé pendant la visite.

A compter de cette visite, le titulaire dispose d'un délai 15 jours ouvrés par défaut (délai différent selon accord avec l'Administration) pour finaliser la VABF et ainsi répondre aux conditions qui resteraient à respecter (levées de réserves, livrables etc.).

Le délai retenu sera consigné dans le procès-verbal afférent, à défaut il correspondra au délai retenu pour la levée des réserves. Une nouvelle visite de validation d'aptitude aura lieu pour finaliser la VABF et axé sur les réserves précédemment mentionnées.

3.2.3 PROCÈS VERBAL DE VALIDATION D'APTITUDE

Le procès-verbal de VABF est établi conjointement par les représentants de l'Administration et le titulaire en s'appuyant sur le document fourni par l'Administration.

Il est établi par système, il y aura autant de procès-verbal que de domaines traités (contrôle d'accès, vidéo protection, intrusion, visiophonie/interphonie).

Le procès-verbal indiquera:

- une vérification d'aptitude sans réserves
- une vérification d'aptitude avec réserves listées- Le rejet

Les réserves seront classées comme suit : bloquante : système inopérant, la réserve impacte la sécurité du site ou l'exploitation du système, les livrables documentaires ne sont pas livrés/validés, les formations n'ont pas été délivrées
non bloquante : la sécurité du site ou l'exploitation du système n'est pas impactée par la réserve

Sur la base du PV, l'Administration se prononcera sur la validation de la VABF avec ou sans réserves ainsi que l'entrée ou non en VSR. Une réserve bloquante ne permet pas d'entrée en VSR.

Une annexe spécifique est à joindre au PV pour consigner la liste des réserves à lever.

Tous les livrables attendus qui n'auraient pas été livrés avant la visite de VABF seront automatiquement consignés comme réserves.

Si le procès-verbal fait état de réserves motivées par des omissions ou des imperfections, le titulaire disposera d'un délai 15 jours ouvrés par défaut (délai différent selon accord avec l'Administration), pour exécuter les travaux nécessaires.

Un PV sera établi à chaque visite de validation d'aptitude.

3.2.4 AJOURNEMENT

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 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.

3.2.5 VSR

L'entrée en VSR constitue la date de mise en service effective du système et correspondra au début de garantie.

La période de vérification de service régulier (VSR) est d'une durée de 30 jours ouvrés à compter de la date de mise en service (cf. PV). 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.

En tout état de cause, la réception définitive n'est effective qu'après constat de la livraison de l'ensemble des documents requis et des prestations réalisées et validées.

3.2.6 RÉCEPTION DÉFINITIVE

La réception définitive de la solution n'est prononcée qu'au terme du processus de réception une fois la période de VSR réalisée.

Le procès-verbal de fin de VSR est alors signé des parties avec le statut et la date de réception définitive. Il sera précisé la date de début de garantie correspondant à l'entrée en VSR et la date de fin de garantie un an après.

Dans le cas où l'Administration serait amenée à prendre possession des installations avant la réception définitive, les installations seront exploitées suivant les instructions de l'entreprise et sous sa responsabilité, sans que cette dernière puisse prétendre à indemnisation.

3.3 GARANTIE

3.3.1 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 dès l'entrée en VSR pour une durée d'un an.

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 défaut par un dispositif de qualité supérieure), 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.

3.3.2 INTERVENTIONS PENDANT LA PÉRIODE DE GARANTIE

3.3.2.1 Astreinte téléphonique

Afin de prendre en compte les incidents, le titulaire devra communiquer un numéro de plateforme téléphonique fonctionnant de 8h à 18h, du lundi au vendredi hors jours fériés et/ou un espace web de ticketing.

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.

Un accusé réception sera envoyé par mail au demandeur.

3.3.2.2 Définition de la gravité de l'incident

Deux niveaux de gravité d'incident sont définis :

- Panne urgente : Une panne urgente correspond à une panne rendant le système complètement inexploitable.
- Panne non urgente : Toutes les autres pannes sont considérées comme non urgentes.

3.3.2.3 Garanties de temps de rétablissement (GTR)

- Panne urgente :

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 8h-17h).

- Panne non urgente :

Elle devra être réparée dans les 72 heures suivant la signalisation de l'incident en heures ouvrables 5 jours sur 7 (du lundi au vendredi 8h-17h).

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).

3.3.3 MISES À JOUR

Pendant la période de garantie, les mises à jour préconisées par le constructeur ou permettant de corriger une anomalie devront être proposées par le titulaire et installées après accord préalable de l'administration. Le titulaire assure une veille fonctionnelle et de sécurité obligatoire sur les produits/logiciels installés.

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).

4 LES EXIGENCES SSI

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 sur décision écrite par l'Administration

Principes de Sécurité des Systèmes d'Information

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

N°	Domaine	Description de la mesure
1	Organisation de la sécurité des SI	Les mots de passe utilisateurs doivent être composés au minimum de 10 caractères alphanumériques, 12 pour les comptes administrateurs.
2	Organisation de la sécurité des SI	L'ensemble des mots de passe devront être changés (camera comprises) et transmis à l'administration par un document informatique et papier.
3	Organisation de la sécurité des SI	Télémaintenance interdite
4	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 lié au renouvellement ;
5	Architecture et exploitation des SI	L'ensemble des équipements sera configuré pour une mise à l'heure centralisée.
6	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.

7	Sécurité physique des locaux	Les équipements seront installés dans des locaux sécurisés
8	Sécurité physique des locaux	Alimentation électrique secourue – onduleur, groupe électrogène – Climatisation – Détection incendie. En cas de coupure électrique, les portes ou portiques devront rester, par défaut, en position fermée.
9	Architecture et exploitation des SI	Respecter les différents profils utilisateurs.
10	Architecture et exploitation des SI Gestion de la continuité des SI	- Sauvegarde hebdomadaire au minimum des données sensibles (clefs de lecture, profil, logs) - Copie physique du disque système à chaque modification importante (stocké dans un local éloigné et sécurisé)
11	Architecture et exploitation des SI	Mettre en place les correctifs de sécurité et upgrade applicatifs matériels
12	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.

13	Architecture et exploitation des SI	Mettre en œuvre un réseau physique dédié aux équipements contribuant à la mise en œuvre des systèmes de sécurisation. Aucune interconnexion ne devra être possible
		entre le RIE et les enclaves « Contrôle d'accès »
14	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)
15	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.
16	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.
17	Architecture et exploitation des SI	Sécuriser les BDD
18	Architecture et exploitation des SI	Respecter le plan d'adressage imposé par le cloisonnement des ressources dans une DMZ
19	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,...)
20	Gestion des autorisations ou accès logique aux ressources	Créer des comptes nominatifs pour les prestataires. Ces comptes devront être supprimés dès la fin de la prestation (cf procédure circuit arrivée/départ)

21	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, ...)
22	Gestion des autorisations ou accès logique aux ressources	Prévoir des badges temporaires
23	Gestion des autorisations ou accès logique aux ressources	Utilisation de comptes nominatifs pour l'authentification des administrateurs. Les comptes nominatifs des prestataires devront être activés/désactivés suivant les besoins d'intervention (cf procédure spécifique compte nominatifs prestataires)
24	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
25	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
26	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
27	Gestion de la continuité des SI	S'assurer de la disponibilité des matériels listés dans les fiches réflexes : (plate-forme de secours, ...),
28	Conformité et contrôle	Respect du « document de référence technique puce sans contact » rédigé par le SHFD