



Secrétariat Général de l'Administration du Ministère de l'Intérieur Sud-Est

*Relogement du service de la DSIC du Ministère de l'Intérieur
Dans le bâtiment "Perspective" de la rue Garibaldi (LYON
03)*

PHASE PROJET
CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
LOT 8 / COURANTS FAIBLES – SURETE



7/7bis rue Abel Hovelacque 75013 PARIS
TEL 01.53.79.04.00 - FAX 01.53.79.06.53
Email : alternet@alternet.net
<http://www.alternet.net/>

Rédacteur : Philippe CULAUD
N° Projet : 240243

Date : 14/04/2026
Version : 4

HISTORIQUE DES INDICES

INDICE	DATE	COMMENTAIRES / MODIFICATIONS
O	05/01/2026	PREMIERE DIFFUSION
1	24/03/2026	MISE A JOUR
2	27/03/2026	MISE A JOUR
3	31/03/2026	MISE A JOUR
4	14/04/2026	MISE A JOUR

SOMMAIRE

CHAPITRE I - GENERALITES	4
I.1. OBJET DU PRESENT DOCUMENT	4
I.2. INSTALLATION EXISTANTE	4
CHAPITRE II - PRESCRIPTIONS GENERALES	5
II.1. PRESTATIONS A LA CHARGE DU LOT CFO-CFA-SSI	5
II.2. CONFIDENTIALITE	5
II.3. DOSSIER D'EXECUTION.....	5
II.4. DOSSIER DES OUVRAGES EXECUTES	6
II.5. RECETTES	6
II.5.1. Contrôles visuels	6
II.5.2. Contrôles fonctionnels	6
II.5.3. Recette courant fort.....	7
II.5.4. Système de contrôle d'accès.....	7
II.5.5. Fiches de recette	7
II.5.6. Procès-verbal de recette	7
CHAPITRE III - PRESCRIPTIONS TECHNIQUES PARTICULIERES	8
III.1. GENERALITES	8
III.2. MATERIELS FOURNIS	8
III.2.1. Equipements centraux	8
III.2.2. Modules déportés	8
III.3. FONCTIONNALITES DU SYSTEME	9
III.4. ORGANES DE VERROUILLAGE.....	10
III.5. CEREMONIE DES CLES	12
III.6. BADGES	13
III.7. CONFORMITE	13
III.8. ESSAIS ET MISE EN SERVICE	14
III.9. CABLAGES ET RACCORDEMENTS	14

CHAPITRE I - GENERALITES

I.1. OBJET DU PRESENT DOCUMENT

Le présent document constitue notre projet visant à définir les travaux techniques « Contrôle d'accès » nécessaires au relogement des services de la DSIC du Ministère de l'Intérieur dans le bâtiment « Perspective » de la rue Garibaldi à LYON (69).

Ce CCTP décrit les prestations d'extension du système de contrôle d'accès existant.

Les 16 locaux à équiper d'un contrôle d'accès sont les suivants :

- SS1
 - o Stockage groupe électrogène
 - o Stockage / décartonnage
- RdC
 - o Stockage EPI
 - o Stockage atelier
 - o Circulation de l'ESR DSIC
 - o Espace ouvert BIS
- R+1
 - o Accès depuis les parties communes (Nb : 4)
 - o Local IGI 13.100
- R+2
 - o Accès depuis les parties communes (Nb : 4)
 - o Local technique DSIC

En complément, il sera mis à disposition de la DSIC un poste d'exploitation, un enrôleur de badge, une imprimante dédiée à la création des badges et un contrôle d'accès CLOUDLINK SYNERGIS.

Ces équipements seront positionnés dans le LT DSIC au niveau R+2.

I.2. INSTALLATION EXISTANTE

Le site est actuellement équipé d'une solution centralisée de contrôle d'accès basée sur la plateforme Genetec Synergis.

Cette solution comprend :

- Un poste client d'exploitation équipé du logiciel Security Desk de Genetec
- Un lecteur encodeur de badge pour l'enrôlement et le paramétrage des badges Desfire EV2
- Des lecteurs de badge STid ARC1, version RS-485 OSDP chiffré fonctionnant en mode transparent et lecture Desfire EV2
- Des modules déportés Secure IO - positionnés dans les gaines techniques – 8 entrées / 8 sorties configurables et communiquant vis RS-485 OSDP
- Un contrôleur d'accès CloudLink Synergis, positionné dans un local technique au R+6

Le CLOUDLINK existant, positionné dans le LT R+6 gère 21 portes sous contrôle d'accès pour un total maximum de 24 portes.

En conséquence, l'entreprise devra la fourniture, la pose et le raccordement d'un CLOUDLINK supplémentaire qui sera positionné dans le LT DSIC au R+2 + liaison catégorie 6A entre le LT R+2 DSIC et le LT R+6.

CHAPITRE II - PRESCRIPTIONS GENERALES

II.1. PRESTATIONS A LA CHARGE DU LOT CFO-CFA-SSI

Sont à la charge du lot CFO-CFA-SSI :

- La fourniture, la pose et le raccordement de l'ensemble des disjoncteurs de protection « haute immunité » nécessaires à l'alimentation des équipements de contrôle d'accès (1 disjoncteur 2x16A 30mA SI/HPI ou équivalent)
- La réalisation des alimentations en câbles U1000 R2V de sections appropriées
Ces câbles seront laissés en attente au droit des équipements à alimenter

NB : L'installation et la configuration du commutateur réseau de l'administration sont à la charge du présent lot.

II.2. CONFIDENTIALITE

Le titulaire s'engage à ne pas divulguer les informations relatives au système d'information du ministère de l'Intérieur dont il a eu connaissance dans le cadre du présent projet, y compris après la fin de sa prestation.

Il est strictement interdit de copier des documents administratifs, quel que soit le moyen utilisé, ou de les conserver en dehors des locaux de la préfecture, sauf autorisation écrite de l'administration.

Il est informé que sa mission peut faire l'objet d'un contrôle de sécurité à tout moment, sans préavis. Il reconnaît également avoir connaissance des sanctions prévues par la loi et les règlements en vigueur en cas de divulgation, volontaire ou par négligence, de ces informations à des personnes non autorisées.

II.3. DOSSIER D'EXECUTION

Le dossier d'exécution fournit par l'Entreprise, 2 semaines avant le début des travaux, devra comporter les documents suivants :

- La nomenclature des plans,
- Les schémas/synoptiques de distribution générale
- La légende avec les marques, le type et la référence des matériels utilisés,
- Les plans côtés de l'équipement des locaux et espaces d'implantations,
- Les plans de canalisation et de repérage des circuits,
- Les plans de détails des gaines et des locaux techniques,
- Les plans de réservations,
- La notice technique des matériels utilisés avec les adresses des fournisseurs,
- Les plans seront fournis à l'échelle 1/50e.

L'ensemble du dossier d'exécution et les aménagements pouvant apparaître en cours de chantier devront être fournis sous forme de plans permettant la synthèse des prestations tous corps d'état.

L'Entreprise prévoira dans son offre, les études de synthèse et l'incidence des modifications entraînées par la synthèse des installations.

Les fichiers seront fournis au standard AUTOCAD.

Les plans et schémas associés aux prestations de l'entreprise devront obligatoirement être conformes aux préconisations du présent CCTP et l'annexe 2 « Principes contrôle d'accès ».

II.4. DOSSIER DES OUVRAGES EXECUTES

Le DOE comprendra l'intégralité de la documentation des équipements installés et sera livré impérativement et au plus tard à la réception du chantier.

A ce titre, l'entreprise complètera le document « Dossier d'Ouvrage Exécuté » du SGAMI.

Il sera livré en format papier (2 exemplaires) et sur support informatique (Clé USB).

Il comprendra notamment :

- Une présentation de l'architecture générale
- Les plans d'implantation de tous les équipements
- Les fiches techniques complètes de l'intégralité des équipements mis en place
- Les schémas et plans de câblage
- Une liste exhaustive des portes contrôlées avec équipements de verrouillage et modules déportés associés
- Les procès-verbaux des tests fonctionnels (vérification du câblage, des accès, de la supervision, du mode dégradé)
- Les certifications de conformité et les attestations de bon fonctionnement (autocontrôles)
- Le PV de réception de l'installation signé

Le contenu détaillé du DOE devra être strictement conforme aux exigences du référentiel ministériel transmis, notamment le modèle-type « DOE Sûreté Bâtiminaire DDPP69 » fourni par la MOA, qui devra être intégralement renseigné et annexé.

II.5. RECETTES

II.5.1. Contrôles visuels

Ils concernent principalement :

- L'étiquetage et le repérage des câbles, lectures et modules déportés
- La conformité de l'installation

II.5.2. Contrôles fonctionnels

Ils comprendront les vérifications suivantes :

- Connectivité complète entre les modules déportés (Secure IO / UTL) et le serveur PREF Corneille
- Vérification de l'adressage IP (adresses assignées aux équipements)
- Tests de supervision des alarmes, pertes de communication, déconnexions et autoprotectons

Conformément à la PSSI et à la note SHFD du 18/05/2017, les éléments suivants devront être vérifiés sur site et documentés :

- Identification et repérage physique des ports des commutateurs (pa sûreté / ports inutilisés) ;
- Blocage des ports USB libres et affectation des ports USB (souris, clavier, ...) sur le poste d'enrôlement en mode utilisateur ;
- Interdiction de tout accès Internet direct ;
- Synchronisation NTP via pare-feux du RIE exclusivement.
- Création des sous-réseaux de contrôle d'accès du SIS (Système d'Information Sûreté) conformément à la note du SHFD. L'entreprise devra installer et configurer le commutateur sûreté fourni par l'administration conformément à l'annexe 1 « Principes câbles équipements raccordement ».

II.5.3. Recette courant fort

- Validation des protections par disjoncteurs différentiel super immunisés
- Test en coupure secteur : maintien de l'alimentation des modules, serveurs, poste client.

II.5.4. Système de contrôle d'accès

- Vérification du fonctionnement de chaque point d'accès (lecteur, verrouillage, alarmes)
- Vérification du paramétrage des plages horaires et profils utilisateurs
- Test d'intégration des cartes SAM (au moins 18 exigences fonctionnelles) ;
- Vérification de la configuration du commutateur (création des vlans, routage) ;
- Vérification au raccordement du RIE ;
- Vérification de l'historisation, remontée d'alarmes, synchronisation NTP ;
- Contrôle de la cérémonie des clés, chiffrement OSDP, badges en mode transparent ;
- Vérification du paramétrage réseau et son raccordement au RIE
- Tests de fonctionnement en mode dégradé suite à perte réseau

II.5.5. Fiches de recette

Elles intégreront :

- Les méthodologies de tests
- Les résultats obtenus (PV signés) sans réserve

II.5.6. Procès-verbal de recette

Un PV de recette sera établi une fois les vérifications effectuées.

CHAPITRE III - PRESCRIPTIONS TECHNIQUES PARTICULIERES

III.1. GENERALITES

Le présent projet prévoit l'extension, aux locaux de la DSIC, du système de contrôle d'accès existant du site (plateforme unifiée Genetec).

L'architecture repose sur un déploiement déporté sécurisé, intégrant des modules STid Secure IO implantés en gaines techniques.

16 points d'accès seront équipés d'un contrôle d'accès avec mise en place systématique de nouveaux organes de verrouillage.

III.2. MATERIELS FOURNIS

III.2.1. Equipements centraux

L'architecture technique repose sur la mise en œuvre de matériels de sûreté hautement sécurisés et conformes aux exigences ANSSI, interopérables avec la plateforme Genetec™ Synergis existante.

Elle inclut notamment :

- Un poste client d'exploitation positionné dans le LT DSIC au R+2, constitué d'un PC de bureau avec les caractéristiques minimales suivantes : Intel i5 / 8 Go RAM / SSD 120 Go, d'un écran 27" Full HD, d'un clavier, d'une souris et des accessoires de fixation
Il sera livré, installé, raccordé et configuré avec le logiciel Security Desk de Genetec™, en environnement Windows 11 Pro. Les performances du poste seront testées en conditions réelles d'exploitation
- Un lecteur encodeur de bureau SECard, en interface USB, permettant l'enrôlement et le paramétrage sécurisé des cartes Desfire EV2 (agents et visiteurs)
Ce lecteur, compatible MIFARE DESFire EV1 à EV3, permettra également la gestion complète des clés via le logiciel SECard, fourni avec licence et documentation
- Une imprimante dédiée aux badges blancs
- 16 lecteurs de badges STid ARC1, version RS-485 OSDP chiffré, avec mode transparent activé et lecture Desfire EV2
- Des modules déportés STid Secure IO, montés sur rail DIN, disposant de 8 entrées / 8 sorties configurables, communiquant via RS-485 OSDP
Chaque module sera alimenté de manière autonome, via des alimentations secourues.
- Un contrôleur d'accès Cloudlink Synergis positionné dans le LT DSIC au R+2 pour les 16 lecteurs

L'ensemble des équipements sera livré avec ses accessoires de montage, fixations, plaques de propreté, et protections mécaniques ou électriques nécessaires à leur bonne intégration.

III.2.2. Modules déportés

Les modules Secure IO pourront être implantés :

- Dans les gaines techniques palières d'étage
- A proximité des portes contrôlées dans la zone sécurisée

Ils seront installés dans des boîtiers à fermeture sécurisée et équipés d'un système d'autoprotection. En cas d'ouverture ou d'arrachement, une alarme sera générée au niveau de la supervision GENETEC.

Aucune donnée sensible ne sera stockée localement dans les modules ou dans leur environnement immédiat.

Les liaisons s'effectueront en bus RS-485 chiffré OSDP, et les alimentations seront secourues avec une autonomie minimale de 3 heures. Les batteries locales seront à fournir par le prestataire.

III.3. FONCTIONNALITES DU SYSTEME

Le système de contrôle d'accès déployé permet notamment :

- L'identification et l'authentification sécurisée des utilisateurs par badge Desfire EV2 (agents CAM) ou Desfire EV1/EV2 (visiteurs), en mode transparent chiffré (OSDP)
- Le déverrouillage des accès après présentation d'un badge valide, avec gestion des plages horaires, des profils d'accès et des niveaux d'autorisation associés
- La surveillance en temps réel de l'état des accès : porte verrouillée, ouverte, forcée, alarme déclenchée, activation d'un DMD (dispositif de demande de sortie)
- Le fonctionnement autonome en mode dégradé : en cas de perte de liaison avec le serveur Corneille, le CloudLink Synergis assure localement la continuité de service et l'accès selon les droits configurés
- La remontée instantanée des événements critiques (ouvertures, anomalies, alarmes, tentatives d'accès invalides) vers le poste de supervision PREF Corneille, via la liaison RIE sécurisée
- L'historisation complète et la traçabilité des événements, avec possibilité de filtrage par accès, utilisateur, groupe, période
- La synchronisation horaire automatique via serveur NTP, garantissant la cohérence temporelle des journaux d'événements
- La supervision des contacts de porte et DM Vert, intégrant à chaque point critique un retour d'état, une LED verte de visualisation et un buzzer sonore de déverrouillage
- La gestion avancée des accès : configuration des droits multizones, scénarios spécifiques, anti-retour, restrictions par créneaux horaires ou par type d'utilisateur
- La protection logicielle renforcée : si un accès à la plateforme centrale est autorisé, activation de l'antivirus McAfee intégré, conforme aux préconisations DITN et SGAMI
- Le chiffrement bout-en-bout des communications entre lecteurs, modules, CloudLink et poste client via le protocole OSDP sécurisé (SAM embarqué, clés certifiées ANSSI)

Toutes ces fonctionnalités seront déclinées pour l'ensemble des portes à contrôler dans le cadre du présent projet.

Elles seront entièrement paramétrables via le logiciel Security Center.

III.4. ORGANES DE VERROUILLAGE

Les organes de verrouillage à mettre en œuvre sont définis en conformité avec les prescriptions de l'ANSSI et les exigences de la DSIC. Tous les équipements devront être pleinement compatibles avec les modules STid Secure IO et s'intégrer nativement à l'architecture du système Genetec™ Synergis.

En complément, l'entreprise devra, pour chaque vantail sous contrôle d'accès, la mise en place et le paramétrage d'un détecteur d'ouverture raccordé sur l'UTL associée.

Le titulaire assurera la fourniture, la pose, le raccordement, la configuration et le paramétrage complet des dispositifs de verrouillage sur les accès identifiés ci-dessous :

- SS1
 - Accès « stockage groupe électrogène »
Mise en place d'une ventouse électromagnétique EF300 (300 kg) en applique avec :
 - Équerres L et Z, contreplaque et support EF300SCP,
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Bouton poussoir de demande de sortie,
 - DM Vert (DMD avec LED verte et buzzer) à 3 contacts,
 - Double contact de porte avec borne de jonction.
 - Accès « Stockage / décartonnage »
Mise en place d'une ventouse électromagnétique EF300 (300 kg) en applique avec :
 - Équerres L et Z, contreplaque et support EF300SCP,
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Bouton poussoir de demande de sortie,
 - DM Vert (DMD avec LED verte et buzzer) à 3 contacts,
 - Contact de porte avec borne de jonction.
- RdC
 - Accès « Stockage EPI » (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction.
 - Stockage atelier (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction.
 - Circulation de l'ESR DSIC (LB en entrée / sortie libre)
Mise en place d'une serrure électrique béquille simple KEL564 axe 50 mm, avec :
 - Béquille inox 70 mm, tête fine inox, plaque de montage,
 - Cylindre ISR6 30x30 mm, variure identique au reste du site,
 - Ferme-porte TS72 avec bras compas,
 - Goulotte d'application avec passe-câble,
 - Contact de porte avec borne de jonction.

- Espace ouvert BIS (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Double contact de porte avec borne de jonction.
- R+1
 - Accès depuis les parties communes (Nb : 4) (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction (dont une à double contact de porte)
 - Local IGI 13.100 (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction.
- R+2
 - Accès depuis les parties communes (Nb : 4) (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction (dont une à double contact de porte)
 - Local technique DSIC (LB en entrée / sortie libre)
Mise en place d'une serrure motorisée KEL518 axe 55mm, avec :
 - Rebond anti-retour,
 - Cylindre profil européen ISR6 2 entrées
 - Ferme-porte TS72 avec bras compas et plaque de montage,
 - Convertisseur 24/48 V vers 12 VDC – 5 A,
 - Résistance du pêne : 1t en poussée
 - Contact de porte avec borne de jonction.

Tous les dispositifs de déverrouillage (DM Vert) doivent permettre une signalisation sonore (buzzer) et visuelle (LED verte) du déverrouillage. Le repérage, le câblage, la protection des circuits et les raccordements seront réalisés conformément au Référentiel VDI, au guide ANSSI et à l'Annexe 1 SGAMI.

Le déverrouillage des DM verts doit remonter à la supervision en évènement « porte forcée ».

Chaque DM vert disposera d'un double contact pour la supervision et son état.

III.5. CEREMONIE DES CLES

La cérémonie des clés du bâtiment DDPP69 est en cours de réalisation.

L'architecture logique GENETEC permettra de différencier les droits d'accès :

- Aux portes communes (entrées du bâtiment, sous-sol) accessibles aux deux entités ;
- Aux portes spécifiques affectées soit à la DDPP, soit au SGAMI-SE.

Cette organisation s'appuiera sur des groupes d'utilisateurs distincts au sein du conteneur « GARIBALDI », avec une gestion différenciée des profils et des droits.

III.6. BADGES

Un conteneur logique unique « GARIBALDI » est mis en place dans Genetec™ Security Center, regroupant l'ensemble des utilisateurs et équipements du site.

A terme, trois groupes fonctionnels distincts y cohabiteront :

- La Préfecture du Rhône (DDPP69) (existant)
- Le SGAMI Sud-Est (SGAMI-SE) (existant)
- **La DSIC (A créer)**

Les portes communes (entrées principales, sous-sols) seront accessibles aux trois entités.

Les autres accès seront affectés selon l'appartenance, avec profils et groupes d'accès distincts dans Genetec™.

Le paramétrage dans Genetec™ comprendra :

- La création du groupe d'accès « DSIC », profils d'utilisateurs, plages horaires et règles anti-passback
- L'affectation logique des lecteurs aux entités et groupes définis
- Le paramétrage sécurisé OSDP des lecteurs

Le système et l'organisation des droits d'accès devront faire l'objet d'une validation par les représentants de la Préfecture.

En complément, l'entreprise fournira 50 badges blancs sécurisés (A confirmer).

III.7. CONFORMITE

L'ensemble du système mis en œuvre répondra aux exigences techniques et réglementaires suivantes :

- ANSSI :
 - o Architecture de contrôle d'accès conforme (CloudLink centralisé, modules Secure IO déportés sans stockage local de données sensibles)
 - o Communication sécurisée via bus RS-485 OSDP v2 chiffré
 - o Intégration de cartes Desfire EV2 (mode transparent avec RandomID)
 - o Gestion sécurisée des clés (SAM AV3, SHA-256, cérémonie de clés double)
- SGAMI Sud-Est :
 - o Conformité avec les prescriptions techniques des annexes 1 à 5 : câblage, topologie, exploitation, supervision
- Normes applicables :
 - o APSAD D83
 - o NF S61-937
 - o NF C 15-100
- Autonomie électrique :
 - o Tous les équipements critiques (modules IO, lecteurs, postes clients) seront connectés à des circuits sécurisés et protégés, avec une autonomie minimale de 3 heures garantie pour chaque alimentation, grâce à des batteries de secours
- Exclusions :
 - o Aucune liaison radio, Wi-Fi, Bluetooth ou non sécurisée n'est tolérée dans l'architecture système
 - o Aucun stockage de badge ou identifiant ne sera autorisé en périphérie sans cryptage validé ANSSI

III.8. ESSAIS ET MISE EN SERVICE

La mise en service opérationnelle du système comprendra l'ensemble des opérations suivantes :

- Tests fonctionnels complets :
 - o Vérification de chaque accès contrôlé (lecteur, verrouillage, état de porte, alarme, bouton poussoir)
 - o Activation des dispositifs DM Vert (buzzer + LED verte)
 - o Contrôle du câblage, repérage, alimentation et communication avec les modules
- Enrôlement des badges :
 - o Création et test des badges CAM (agents Préfecture et SGAMI), badges visiteurs ;
 - o Vérification du fonctionnement en mode transparent avec RandomID ;
 - o Enregistrement dans Genetec™ avec affectation des droits et groupes.
- Validation des scénarios et profils :
 - o Contrôle des plages horaires, droits différenciés, anti-retour, alarmes ;
 - o Vérification du bon fonctionnement des profils spécifiques (DSIC, visiteurs).

III.9. CABLAGES ET RACCORDEMENTS

Le câblage du système de contrôle d'accès sera conforme aux prescriptions de sécurité en vigueur, notamment :

- Référentiel VDI SGAMI
- SGAMI SE – Annexe 1 : Principe de câblage des équipements
- Guide ANSSI – Contrôle d'accès physique sécurisé (version applicable au moment des études d'exécution)

Prescriptions générales :

- Tous les câbles de données (RS-485, Ethernet, DM Vert, alimentation) seront posés en un seul tenant
- Les câbles seront posés dans des chemins techniques fermés, fourreaux ou goulottes apparentes
- Les traversées de murs ou planchers seront gainées, étanchées CF ou RF selon directives du MOE
- Les distances minimales entre courants forts et faibles seront rigoureusement respectées (30 cm en parallèle, 5 cm en croisement)

Repérage :

- Chaque câble sera repéré à ses deux extrémités selon un code unique (ex. : CA6-L, CA6-CF, CA6-IO)
- Un registre de repérage (tableau Excel) sera fourni au DOE, identifiant tous les câbles, leurs extrémités, usage, type et longueur estimée

Prescriptions spécifiques :

- Le câblage RS-485 (bus OSDP sécurisé) sera réalisé en topologie linéaire, avec terminaison active, depuis le CloudLink R+6 vers les modules Secure IO
- Les câbles de puissance seront protégés par des disjoncteurs différentiels 30mA type HI (haute immunité) en tête de ligne
- Tous les équipements critiques (modules IO, lecteurs, postes clients) seront connectés à des circuits sécurisés et protégés, avec une autonomie minimale de 3 heures garantie pour chaque alimentation, grâce à des batteries de secours
- Un plan de câblage complet sera intégré au DOE : il détaillera le routage physique et logique, les points de raccordement, les types de câbles et protections utilisées
- Les fiches de test de continuité, d'isolement et de repérage seront jointes et signées