DOSSIER DE CONSULTATION DES ENTREPRISES
CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

ANNEXE 3 : MESURES DE CYBERSÉCURITÉ - NOTICE

Table des matières

1. Objet et principes généraux....4
Vérification de la conformité de la solution....4
Engagements du candidat et prise en compte du niveau de maturité de la solution....4
Notation....5
2. Architecture d'identité et de confiance....7
SEC-01 — Authentification des utilisateurs par OIDC....7
SEC-02 — Gestion des rôles et des privilèges....7
SEC-03 — Authentification réseau IEEE 802.1X avec EAP-TLS....7
SEC-04 — Protection des clés privées....8
SEC-05 — ACME et gestion du cycle de vie des certificats....8
SEC-06 — Sécurisation du canal de pilotage par TLS avec authentification mutuelle....9
SEC-07 — Sécurisation de l'interface Web....10
SEC-08 — Séparation des certificats selon leur usage....10
3. Réduction de la surface d'attaque....12
SEC-09 — Désactivation des services inutiles....12
SEC-10 — Gestion d'IPv4 et IPv6....12
SEC-11 — Comptes et mots de passe par défaut....12
4. Pare-feu et filtrage réseau....13
SEC-12 — Pare-feu intégré....13
SEC-13 — Journalisation du filtrage....13
SEC-14 — Moindre privilège réseau....13
5. Communications sécurisées....14
SEC-15 — Versions et configuration TLS....14
SEC-16 — Ports de communication configurables....14
6. Administration et accès....15
SEC-17 — Administration SSH....15
SEC-18 — Protection contre les attaques par force brute....15
SEC-19 — Interdiction de la connexion root distante....15
SEC-20 — Expiration des sessions....15
SEC-21 — Compte local de secours....15
SEC-22 — Politique de mots de passe....16
7. Traçabilité, journalisation et supervision....17
SEC-23 — Synchronisation temporelle....17
SEC-24 — Journalisation des événements de sécurité....17
SEC-25 — Supervision SNMP....17
SEC-26 — Traçabilité des modifications....18
SEC-27 — Export des journaux....18
SEC-28 — Protection des journaux....18
8. Maintenance et interfaces locales....19
SEC-29 — Protection des interfaces locales de maintenance....19
SEC-30 — Désactivation des interfaces de maintenance....19
9. Firmware, démarrage sécurisé et résilience....20
SEC-31 — Firmware signé....20
SEC-32 — Vérification du firmware avant installation....20
SEC-33 — Secure Boot....20
SEC-34 — Protection contre le rollback....20
SEC-35 — Récupération après incident....20
10. Maintien en condition de sécurité....21

SEC-36 — Gestion des vulnérabilités....21
SEC-37 — Correctifs de sécurité....21
SEC-38 — Fin de support....21
SEC-39 — SBOM....21
11. Sauvegarde, restauration et documentation....22
SEC-40 — Sauvegarde sécurisée de la configuration....22
SEC-41 — Restauration sécurisée....22
SEC-42 — Documentation de sécurité....22
SEC-43 — Mesures de cybersécurité complémentaires....22

1. Objet et principes généraux

Le titulaire devra garantir un niveau de cybersécurité adapté à l'exploitation de panneaux à messages variables (PMV) raccordés au système de supervision et de pilotage de l'exploitant.

Les équipements devront être conçus et configurés selon les principes suivants :

- moindre privilège ;
- réduction de la surface d'attaque ;
- défense en profondeur ;
- sécurisation des communications ;
- séparation des privilèges ;
- traçabilité des actions ;
- maintien en condition de sécurité pendant toute leur durée d'exploitation.

Les fonctions de cybersécurité ne devront pas dégrader les fonctions opérationnelles du PMV.

Sauf indication contraire dans le présent marché, les fonctions de sécurité devront être configurables à distance de manière sécurisée. Les paramètres de sécurité devront être conservés après redémarrage de l'équipement.

Le titulaire devra fournir les éléments permettant de démontrer la conformité de la solution aux exigences du présent chapitre, notamment au moyen de la documentation constructeur, de la matrice de conformité et, lors de la recette, d'essais fonctionnels réalisés sur un PMV représentatif de la solution proposée.

Vérification de la conformité de la solution

La DIR pourra demander la mise à disposition d'une unité centrale de test ou d'un équipement représentatif de la solution proposée au cours de l'analyse des offres ainsi qu'à l'issue de la première année d'exécution du marché.

Ces équipements pourront être utilisés par la DIR afin de vérifier, au moyen d'essais, de démonstrations et, le cas échéant, de vérifications techniques, la conformité de la solution aux exigences de cybersécurité du présent chapitre et la cohérence des réponses apportées par le candidat dans sa matrice de conformité.

Le candidat s'engage à répondre aux sollicitations de la DIR nécessaires à la réalisation de ces vérifications lors de ces deux périodes et à mettre à disposition les moyens techniques nécessaires à la réalisation des essais.

Les modalités pratiques, la durée et les conditions de réalisation de ces essais seront définies par la DIR en fonction des vérifications à effectuer.

Engagements du candidat et prise en compte du niveau de maturité de la solution

Pour chaque exigence de cybersécurité du présent chapitre, le candidat devra apporter une réponse dans les colonnes **« 2026 »** et **« 2027 »** de la matrice de conformité.

Dans la colonne **« 2026 »**, le candidat décrira le niveau de conformité de la solution proposée à la date de remise de l'offre. Il précisera, le cas échéant, les conditions de mise en œuvre, de configuration ou d'intégration nécessaires à l'obtention de ce niveau de conformité.

Dans la colonne **« 2027 »**, le candidat décrira le niveau de conformité que la solution atteindra au plus tard le **31 décembre 2027**. Lorsque ce niveau de conformité nécessite une évolution ou un développement, le candidat devra préciser notamment le principe de la solution envisagée, les principales évolutions nécessaires ainsi que, le cas échéant, les conditions ou dépendances techniques associées.

Les réponses apportées par le candidat dans les colonnes **« 2026 »** et **« 2027 »** constituent des engagements contractuels du titulaire.

Le titulaire s'engage à réaliser les évolutions et développements nécessaires à l'atteinte, au plus tard le **31 décembre 2027**, du niveau de conformité déclaré dans la matrice de conformité.

Les évolutions réalisées ne devront pas dégrader les fonctionnalités opérationnelles du PMV, le niveau de sécurité de la solution ni le niveau de conformité atteint au titre des autres exigences de cybersécurité.

La conformité déclarée pour chacune des échéances devra pouvoir être vérifiée par la DIR au moyen notamment de la documentation fournie, de démonstrations, d'essais fonctionnels ou de vérifications techniques.

Notation

La notation de chaque exigence sera effectuée sur la base du nombre maximal de points qui lui est attribué dans la grille de notation.

Pour chaque exigence, la notation est établie selon deux échéances :

- **2026 :** la note maximale correspond à **100 % des points** attribués à l'exigence ;
- **2027 :** la note maximale correspond à **50 % des points** attribués à l'exigence en 2026.

La note attribuée à chaque échéance est déterminée au regard du niveau de conformité décrit par le candidat dans la matrice de conformité et des éléments justificatifs fournis.

Une solution satisfaisant totalement une exigence dès **2026** pourra obtenir **100 % de la note 2026** et donc **100 % de la note 2027**.

Lorsqu'une solution ne satisfait que partiellement une exigence en **2026**, le niveau de conformité effectivement atteint sera pris en compte dans l'attribution de la note 2026. Si le candidat s'engage à atteindre un niveau de conformité supérieur au plus tard le **31 décembre 2027**, le niveau de conformité alors déclaré sera pris en compte pour l'attribution de la note **2027**.

L'appréciation des réponses tiendra notamment compte :

- du niveau réel de conformité de la solution à chacune des échéances ;
- de la précision et de la qualité des éléments fournis ;
- des éventuelles conditions de mise en œuvre, de configuration ou d'intégration ;
- pour les évolutions prévues en 2027, de la précision de l'engagement, de la crédibilité du développement envisagé et de la maturité de la solution proposée.

L'absence d'éléments suffisamment précis permettant d'apprécier le niveau de conformité déclaré pourra conduire à une réduction de la note attribuée à l'exigence concernée.

---

2. Architecture d'identité et de confiance

SEC-01 — Authentification des utilisateurs par OIDC

Le PMV devra supporter l'authentification des utilisateurs au moyen du protocole **OIDC (OpenID Connect)** auprès d'un fournisseur d'identité externe.

L'interface d'administration du PMV devra permettre de configurer les paramètres nécessaires à l'utilisation du fournisseur d'identité, notamment :

- l'identifiant du fournisseur d'identité ;
- les paramètres du client OIDC ;
- les autorités de certification ou mécanismes de confiance nécessaires ;
- les paramètres d'authentification et de session ;
- les informations nécessaires à la récupération des identités et attributs utilisateurs.

Le PMV devra être en mesure d'utiliser les informations fournies par le fournisseur d'identité pour déterminer les droits de l'utilisateur conformément à SEC-02.

SEC-02 — Gestion des rôles et des privilèges

Le PMV devra mettre en œuvre un contrôle d'accès fondé sur les rôles (RBAC).

A minima, les droits devront permettre de distinguer les fonctions suivantes :

- consultation ;
- exploitation ;
- administration/maintenance.

Les droits associés à chaque rôle devront être configurables ou, à défaut, clairement documentés par le titulaire.

Un utilisateur ne devra disposer que des privilèges nécessaires à l'exercice de sa fonction.

Le PMV devra permettre l'association des utilisateurs ou groupes issus du fournisseur d'identité OIDC aux rôles applicatifs du PMV.

SEC-03 — Authentification réseau IEEE 802.1X avec EAP-TLS

Le PMV devra supporter **IEEE 802.1X avec EAP-TLS** pour son authentification auprès de l'infrastructure réseau.

L'utilisation d'une authentification reposant uniquement sur une identité et un mot de passe ne pourra pas se substituer à l'authentification EAP-TLS requise.

Le PMV devra permettre la configuration des paramètres nécessaires à son authentification, notamment :

- le certificat client utilisé pour EAP-TLS ;
- l'autorité de certification de confiance ;
- les paramètres EAP-TLS ;
- les paramètres nécessaires à l'identification du serveur d'authentification ;
- les paramètres nécessaires au renouvellement ou au remplacement du certificat.

Le fonctionnement du PMV devra être compatible avec une architecture dans laquelle le commutateur d'accès réalise l'authentification 802.1X et applique ensuite les droits d'accès réseau définis par l'infrastructure de contrôle d'accès.

Le titulaire devra documenter les échanges nécessaires entre le PMV, le commutateur d'accès et l'infrastructure d'authentification.

SEC-04 — Protection des clés privées

Les clés privées utilisées par les mécanismes cryptographiques du PMV devront être protégées contre tout accès, extraction ou utilisation non autorisés.

Sont notamment concernées les clés privées utilisées pour :

- l'authentification du PMV sur le réseau au moyen de 802.1X/EAP-TLS ;
- la sécurisation du canal de pilotage au moyen de TLS ;
- la sécurisation des communications HTTPS, lorsque celles-ci sont directement terminées par le PMV ;
- la sécurisation des communications avec un reverse proxy au moyen de TLS avec authentification mutuelle, lorsque cette fonction est mise en œuvre.

Les clés privées critiques devront être protégées par un **TPM 2.0, un Secure Element ou un mécanisme matériel offrant un niveau de protection équivalent**.

Les clés privées critiques devront être non exportables depuis le composant de sécurité.

Le titulaire devra décrire dans son dossier technique :

- le mécanisme matériel utilisé ;
- les clés privées concernées ;
- les fonctions auxquelles elles sont associées ;
- les mécanismes de génération, de stockage et d'utilisation des clés ;
- les mesures mises en œuvre pour empêcher leur extraction ou leur utilisation non autorisée.

SEC-05 — ACME et gestion du cycle de vie des certificats

Le PMV devra supporter **ACME (Automatic Certificate Management Environment)** pour l'enrôlement et le renouvellement automatisé des certificats utilisés par ses fonctions de sécurité.

L'adresse du service ACME devra être configurable.

Le mécanisme devra permettre au minimum :

- l'enrôlement initial des certificats ;
- le renouvellement automatique avant expiration ;
- la définition d'un seuil configurable avant expiration ;
- la génération ou l'utilisation sécurisée de la clé privée associée ;
- l'installation automatique du nouveau certificat ;
- la conservation du certificat actuellement valide jusqu'à validation du nouveau certificat ;
- la détection des erreurs d'enrôlement ou de renouvellement ;
- les nouvelles tentatives automatiques ;
- la journalisation des opérations ;
- la signalisation des échecs.

Aucune intervention physique sur le PMV ne devra être nécessaire pour le renouvellement nominal d'un certificat.

Le mécanisme devra permettre le remplacement d'un certificat devenu compromis, invalide ou révoqué.

Le titulaire devra préciser les mécanismes mis en œuvre pour gérer l'expiration, l'invalidation et le remplacement des certificats.

SEC-06 — Sécurisation du canal de pilotage par TLS avec authentification mutuelle

Les communications de pilotage entre le frontal de communication de l'exploitant et le PMV devront être protégées contre l'écoute, l'altération et l'usurpation.

Le canal de pilotage devra être sécurisé au moyen de **TLS avec authentification mutuelle des deux extrémités au moyen de certificats**.

Cette fonction pourra être mise en œuvre au niveau du protocole applicatif ou au moyen d'une couche de sécurisation dédiée telle que **stunnel**, ou d'un mécanisme équivalent offrant un niveau de sécurité au moins équivalent.

Lorsque stunnel est utilisé, il devra assurer la terminaison du canal TLS entre le frontal de communication et le PMV.

Le PMV devra vérifier la validité et la chaîne de confiance du certificat présenté par le frontal de communication.

Le frontal de communication devra réciproquement vérifier la validité et la chaîne de confiance du certificat présenté par le PMV.

Les autorités de certification de confiance devront être configurables.

Lorsque le protocole de pilotage applicatif ne met pas lui-même en œuvre le chiffrement et l'authentification, le service applicatif protégé ne devra pas être directement accessible depuis le réseau sur son port applicatif.

Les certificats utilisés pour le canal de pilotage devront pouvoir être renouvelés et remplacés conformément aux mécanismes de gestion des certificats prévus au présent CCTP.

Le titulaire devra préciser dans sa réponse les éléments suivants :

- le protocole de pilotage concerné ;
- le ou les ports utilisés ;
- le mécanisme de terminaison TLS ;
- les certificats utilisés par chacune des extrémités ;
- le mécanisme de vérification de la chaîne de confiance ;
- le chemin de communication entre le frontal, le mécanisme de sécurisation et l'application de pilotage du PMV.

SEC-07 — Sécurisation de l'interface Web

L'interface Web d'administration du PMV devra être accessible exclusivement au moyen de **HTTPS**.

Les communications entre un composant intermédiaire de type **reverse proxy** et le PMV pourront être sécurisées au moyen de TLS avec authentification mutuelle des extrémités.

Lorsque le PMV supporte l'authentification mutuelle TLS pour son interface Web, cette fonction devra permettre au PMV de vérifier l'identité du composant client autorisé et au composant client de vérifier l'identité du PMV.

Les autorités de certification de confiance devront être configurables.

Les certificats utilisés pour l'interface Web devront pouvoir être gérés conformément au mécanisme de gestion du cycle de vie des certificats défini en SEC-05.

Le titulaire devra préciser dans sa réponse :

- le mécanisme de sécurisation de l'interface Web ;
- le point de terminaison TLS ;
- les certificats utilisés ;
- la possibilité de mettre en œuvre une authentification mutuelle TLS ;
- les modalités de vérification de l'identité du PMV par un reverse proxy ou un client d'administration ;
- les modalités de gestion et de renouvellement des certificats.

Lorsque l'architecture proposée repose sur un reverse proxy, le titulaire devra décrire le périmètre exact des communications sécurisées entre le reverse proxy et le PMV.

SEC-08 — Séparation des certificats selon leur usage

Le PMV devra permettre l'utilisation de certificats et de clés distincts pour les différents usages de sécurité, notamment :

- authentification 802.1X/EAP-TLS ;
- sécurisation du canal de pilotage ;
- sécurisation de l'interface Web ;
- authentification mutuelle TLS avec un reverse proxy, lorsque cette fonction est mise en œuvre.

Les certificats et clés utilisés pour des usages distincts devront pouvoir être gérés indépendamment lorsque l'architecture de sécurité le nécessite.

Le titulaire devra préciser dans sa réponse :

- les certificats utilisés par chaque fonction ;
- les usages associés à chaque certificat ;
- les autorités de certification utilisées ;
- les modalités d'enrôlement et de renouvellement ;
- les mécanismes de protection des clés privées associées.

L'utilisation d'un même certificat pour plusieurs fonctions de sécurité devra être justifiée par le titulaire et ne devra pas conduire à une dégradation du niveau de sécurité ou à une impossibilité de gérer indépendamment le cycle de vie des identités concernées.

---

3. Réduction de la surface d'attaque

SEC-09 — Désactivation des services inutiles

Tout service, protocole ou fonctionnalité réseau non nécessaire au fonctionnement du PMV devra pouvoir être désactivé.

La liste des services activés par défaut devra être documentée.

SEC-10 — Gestion d'IPv4 et IPv6

IPv6 pourra être désactivé lorsqu'il n'est pas nécessaire au fonctionnement du PMV.

Lorsque IPv6 est activé, les mêmes exigences de sécurité que pour IPv4 devront être appliquées, notamment en matière de filtrage réseau, d'administration et de sécurisation des communications.

Le titulaire devra documenter les services accessibles en IPv4 et IPv6.

SEC-11 — Comptes et mots de passe par défaut

Aucun compte administrateur ou mot de passe commun à l'ensemble des PMV ne devra être fourni.

Les identifiants et secrets nécessaires à la mise en service devront être protégés et ne devront pas constituer des identifiants permanents communs à tous les équipements.

---

4. Pare-feu et filtrage réseau

SEC-12 — Pare-feu intégré

Le PMV devra intégrer un pare-feu permettant de contrôler les flux réseau entrants et sortants.

Le filtrage devra pouvoir être réalisé selon au minimum :

- adresse source ;
- adresse destination ;
- protocole ;
- port source et destination ;
- direction du flux.

La politique par défaut devra être configurable en **ACCEPT ou DENY**.

La configuration du pare-feu devra être persistante après redémarrage du PMV.

SEC-13 — Journalisation du filtrage

Le pare-feu devra permettre la journalisation des événements de filtrage, notamment des connexions refusées.

Les informations journalisées devront permettre, lorsque techniquement disponible, d'identifier au minimum la date et l'heure, les adresses concernées, le protocole, les ports et l'action appliquée.

Les événements devront pouvoir être transmis au mécanisme de journalisation distant prévu au présent chapitre.

SEC-14 — Moindre privilège réseau

Le titulaire devra documenter l'ensemble des flux réseau nécessaires au fonctionnement du PMV et des fonctions de sécurité associées.

La configuration du PMV devra permettre de limiter les communications aux seuls flux nécessaires au fonctionnement et à l'administration autorisée de l'équipement.

---

5. Communications sécurisées

SEC-15 — Versions et configuration TLS

TLS 1.2 au minimum devra être supporté.

TLS 1.3 devra être supporté lorsque compatible avec les composants logiciels et matériels concernés.

SSL ainsi que TLS 1.0 et TLS 1.1 devront être désactivés.

Les suites cryptographiques faibles ou obsolètes devront pouvoir être désactivées.

SEC-16 — Ports de communication configurables

Les ports utilisés par les services d'administration et de communication devront être configurables lorsque cette possibilité est techniquement pertinente.

La liste des ports ouverts par défaut devra être fournie par le titulaire.

---

6. Administration et accès

SEC-17 — Administration SSH

Lorsque SSH est utilisé, seule la version **SSHv2** devra être supportée.

L'authentification par clé devra être supportée.

L'authentification par mot de passe devra pouvoir être désactivée.

Le service SSH devra pouvoir être désactivé lorsqu'il n'est pas nécessaire.

SEC-18 — Protection contre les attaques par force brute

Les mécanismes d'authentification devront intégrer des mesures de protection contre les tentatives répétées d'authentification.

Ces mesures devront comprendre au minimum une ou plusieurs des fonctions suivantes :

- limitation du nombre de tentatives ;
- temporisation progressive ;
- verrouillage temporaire ;
- délai entre les tentatives ;
- journalisation des tentatives.

Les paramètres applicables devront être documentés.

SEC-19 — Interdiction de la connexion root distante

La connexion directe au compte root devra être interdite sur les interfaces d'administration accessibles à distance.

Les opérations nécessitant des privilèges élevés devront utiliser un mécanisme d'élévation de privilèges contrôlé et traçable.

SEC-20 — Expiration des sessions

Les sessions d'administration devront pouvoir être automatiquement interrompues après une durée d'inactivité configurable.

SEC-21 — Compte local de secours

Un mécanisme d'accès local de secours devra être prévu afin de permettre la récupération de l'équipement en cas d'indisponibilité du fournisseur d'identité.

Cet accès devra :

- être distinct du mécanisme d'administration nominal via OIDC ;
- être protégé par une authentification forte adaptée ;

- être limité aux opérations nécessaires à la récupération ou à la maintenance ;
- être journalisé.

Le titulaire devra décrire le mécanisme de secours.

SEC-22 — Politique de mots de passe

Lorsqu'un mot de passe est utilisé, sa politique devra être configurable en matière de :

- longueur minimale ;
- complexité ;
- historique lorsque supporté ;
- nombre de tentatives autorisées.

Les caractères ASCII imprimables devront être acceptés.

Le système ne devra pas tronquer silencieusement les mots de passe.

---

7. Traçabilité, journalisation et supervision

SEC-23 — Synchronisation temporelle

Le PMV devra supporter la synchronisation de son horloge au moyen de **NTP ou d'un mécanisme équivalent,** avec une source de temps configurable.

SEC-24 — Journalisation des événements de sécurité

Le PMV devra journaliser, **lorsqu'ils sont applicables à la solution proposée et effectivement mis en œuvre**, les événements de sécurité suivants :

- les authentifications réussies et échouées ;
- les modifications de configuration ;
- les modifications de messages et de programmes ;
- les événements relatifs à 802.1X/EAP-TLS ;
- les événements relatifs aux certificats et à la PKI ;
- les événements du pare-feu ;
- les opérations de maintenance ;
- les mises à jour du firmware ;
- les redémarrages ;
- les événements système significatifs.

La journalisation devra porter sur les fonctions et mécanismes effectivement présents et activés sur le PMV.

L'absence d'un mécanisme, protocole ou fonction dans la solution proposée ne pourra pas, à elle seule, être considérée comme un défaut de journalisation de l'événement correspondant.

Le candidat devra préciser, dans sa réponse, les événements effectivement journalisés par la solution et, le cas échéant, les limites de journalisation identifiées.

SEC-25 — Supervision SNMP

Le PMV devra, lorsqu'une fonction de supervision SNMP est mise en œuvre, prendre en charge **SNMPv3** pour les échanges avec le système de supervision de l'exploitant.

L'utilisation de versions antérieures de SNMP, notamment SNMPv1 et SNMPv2c, devra pouvoir être désactivée.

SNMPv3 devra permettre, selon les besoins de l'exploitation, l'utilisation des mécanismes de sécurité appropriés, notamment l'authentification et le chiffrement des échanges.

Le PMV devra permettre la supervision au minimum des informations nécessaires au suivi de son état de fonctionnement et de sa disponibilité.

Lorsqu'une infrastructure de certificats est mise en œuvre sur le PMV, celui-ci devra permettre de superviser l'état de validité des certificats utilisés par l'équipement et, lorsque l'information est

techniquement disponible, leur **date d'expiration**. Cette information devra pouvoir être exploitée par le système de supervision afin de permettre l'identification anticipée des certificats arrivant à expiration.

Le candidat précisera dans sa matrice de conformité :

- la version ou les versions de SNMP supportées ;
- les mécanismes de sécurité disponibles avec SNMPv3 ;
- les informations de supervision accessibles ;
- les MIB ou OID disponibles pour la supervision ;
- les informations relatives aux certificats accessibles par SNMP, notamment leur date d'expiration ;
- les éventuelles limitations ou dépendances nécessaires à la mise en œuvre.

SEC-26 — Traçabilité des modifications

Toute modification d'un message, programme ou paramètre d'exploitation devra permettre d'identifier au minimum :

- l'utilisateur ayant réalisé l'action ;
- la date et l'heure ;
- l'action réalisée ;
- l'objet modifié.

Lorsque techniquement possible, l'événement devra également conserver l'ancienne et la nouvelle valeur.

Les opérations réalisées par un compte de secours ou un compte de maintenance privilégié devront être identifiables.

SEC-27 — Export des journaux

Les événements de sécurité devront pouvoir être exportés vers un serveur **Syslog distant** ou une infrastructure SIEM.

Le mécanisme d'export devra être documenté par le titulaire.

SEC-28 — Protection des journaux

Les journaux de sécurité devront être protégés contre leur modification ou suppression non autorisée.

---

8. Maintenance et interfaces locales

SEC-29 — Protection des interfaces locales de maintenance

Toute interface locale permettant d'accéder aux fonctions de maintenance ou d'administration du PMV devra être protégée par authentification.

SEC-30 — Désactivation des interfaces de maintenance

Les interfaces de maintenance qui ne sont pas nécessaires à l'exploitation devront pouvoir être désactivées.

Le titulaire devra documenter les interfaces concernées et leur état par défaut.

---

9. Firmware, démarrage sécurisé et résilience

SEC-31 — Firmware signé

Les mises à jour firmware devront être signées numériquement par une chaîne de confiance maîtrisée par le constructeur.

SEC-32 — Vérification du firmware avant installation

La signature et l'intégrité du firmware devront être vérifiées avant son installation.

Un firmware dont la signature est absente, invalide ou dont l'intégrité est compromise devra être refusé.

SEC-33 — Secure Boot

Le PMV devra mettre en œuvre un mécanisme de **Secure Boot** permettant de vérifier, lors du démarrage, l'authenticité et l'intégrité des composants logiciels nécessaires au fonctionnement du PMV.

Tout composant logiciel ne satisfaisant pas les contrôles de sécurité devra être refusé ou empêcher le démarrage normal de l'équipement.

SEC-34 — Protection contre le rollback

Le PMV devra empêcher ou contrôler le retour vers une version firmware connue comme vulnérable ou non autorisée.

Le mécanisme mis en œuvre devra être documenté.

SEC-35 — Récupération après incident

Le PMV devra disposer d'un mécanisme permettant sa récupération après :

- une mise à jour firmware échouée ;
- une corruption logicielle ;
- une interruption pendant une opération de mise à jour.

Le mécanisme de récupération ne devra pas permettre de contourner les mécanismes de sécurité du PMV.

---

10. Maintien en condition de sécurité

SEC-36 — Gestion des vulnérabilités

Le titulaire devra assurer une veille de sécurité pendant toute la durée contractuelle applicable à la solution.

Le titulaire devra informer l'exploitant des vulnérabilités affectant les composants matériels ou logiciels du PMV susceptibles d'avoir un impact sur la sécurité de la solution.

Le titulaire devra proposer les correctifs ou mesures compensatoires nécessaires.

Les modalités de notification, de qualification et de traitement des vulnérabilités devront être documentées.

SEC-37 — Correctifs de sécurité

Le titulaire devra fournir les correctifs de sécurité nécessaires pendant la durée de support contractuelle.

Les modalités de distribution, d'installation et de vérification des mises à jour de sécurité devront être documentées.

Les mises à jour de sécurité devront conserver les mécanismes de signature et de vérification prévus au présent CCTP.

SEC-38 — Fin de support

Le titulaire devra informer l'exploitant suffisamment en amont de toute fin de support ou de maintenance de la version matérielle ou logicielle fournie.

Le titulaire devra préciser les conditions de maintien en sécurité de la solution jusqu'à son remplacement.

SEC-39 — SBOM

Le titulaire devra fournir une **Software Bill of Materials (SBOM)** décrivant les composants logiciels intégrés au PMV.

La SBOM devra être fournie dans un format standard reconnu, notamment **SPDX, CycloneDX ou format équivalent documenté**.

Elle devra être maintenue à jour en cas d'évolution significative des composants logiciels.

---

11. Sauvegarde, restauration et documentation

SEC-40 — Sauvegarde sécurisée de la configuration

Le PMV devra permettre la sauvegarde de sa configuration dans un format permettant sa restauration sur l'équipement ou sur un équipement de remplacement compatible.

Les fichiers de sauvegarde devront être protégés contre les modifications non autorisées.

Les mots de passe, clés privées et autres secrets ne devront pas être exportés en clair dans les fichiers de sauvegarde.

Les opérations de sauvegarde devront être authentifiées et, lorsqu'elles sont réalisées par un utilisateur, journalisées.

SEC-41 — Restauration sécurisée

Le PMV devra permettre la restauration de sa configuration à partir d'une sauvegarde préalablement autorisée.

La restauration devra être authentifiée.

Les opérations de restauration devront être journalisées.

La restauration d'une configuration ne devra pas permettre de contourner les mécanismes de sécurité ou de réintroduire des paramètres interdits.

SEC-42 — Documentation de sécurité

Le titulaire devra fournir une documentation permettant l'administration et l'exploitation sécurisées du PMV.

SEC-43 — Mesures de cybersécurité complémentaires

Le candidat pourra proposer des mesures, mécanismes, fonctions, prestations ou résultats d'audit externe de cybersécurité, accompagnés le cas échéant des mesures correctives mises en œuvre ou prévues, qui ne font pas explicitement l'objet d'une exigence du présent chapitre, dès lors qu'ils apportent un niveau de sécurité supplémentaire ou renforcent la protection du PMV et de son environnement d'exploitation.

Les propositions pourront notamment comprendre la réalisation d'un test d'intrusion, d'un audit de cybersécurité ou d'une évaluation de sécurité indépendante, ainsi que les mesures de correction ou de remédiation qui en résultent.

Le candidat devra décrire :

- la mesure proposée et son principe de fonctionnement ou, pour un audit, son périmètre et sa méthodologie ;

- les menaces ou risques auxquels elle répond ;
- son périmètre d'application ;
- ses modalités d'intégration à l'architecture proposée ;
- ses éventuelles contraintes ou prérequis d'exploitation ;
- pour un audit ou un test d'intrusion, sa date de réalisation, son niveau d'indépendance, les principaux résultats obtenus et, le cas échéant, les mesures correctives mises en œuvre ou prévues. La DIR s’engage à ne diffuser aucun document sensible.

Ces mesures pourront notamment concerner la protection du PMV, des communications, des accès, des données, du firmware, de l'administration, de la détection d'événements de sécurité ou du maintien en condition de sécurité.

La notation portera notamment sur la pertinence, l'efficacité, le caractère opérationnel, le niveau de maturité et le caractère vérifiable des mesures proposées ou des résultats présentés.

Pour les audits, tests d'intrusion ou évaluations de sécurité, la notation tiendra notamment compte de la pertinence du périmètre, de la méthodologie employée, de l'indépendance de l'évaluation, de sa récence, des résultats obtenus et de la prise en compte effective des éventuelles vulnérabilités identifiées.

Les mesures proposées ne pourront pas se substituer aux exigences du présent chapitre ni être considérées comme compensant une réponse insuffisante à une autre exigence.