



TERMES DE RÉFÉRENCE (TDR)

TDR-CGA/SPAT/2026

**SMART GATE P1 – P2 – SYSTÈME INTELLIGENT DE CONTRÔLE
ET GESTION DES ACCÈS PORTUAIRES**

CONTEXTE ET JUSTIFICATION DU PROJET

I-1 Contexte général

Le Port de Toamasina est la principale infrastructure portuaire de Madagascar, assurant plus de 80 % du commerce extérieur du pays. En tant qu'installation portuaire au sens du Code ISPS / SOLAS 1974 amendé, le port est soumis à des exigences strictes en matière de contrôle d'accès, de protection périmétrique et de traçabilité des mouvements des personnes, des motocyclettes et des véhicules.

Les portails P1 et P2 constituent les points d'accès stratégiques de l'enceinte portuaire. Ils représentent les zones de convergence des flux de personnes (agents portuaires, visiteurs, usagers portuaires, prestataires extérieurs), de véhicules et de marchandises. Leur sécurisation efficace est indispensable à la conformité du port aux standards internationaux et à la protection de l'ensemble de l'enceinte contre les intrusions et les actes malveillants.

Le présent marché matérialise la première étape de la vision SPAT 2.0 : doter le port d'un système de contrôle d'accès intelligent, conçu comme brique fondatrice d'un écosystème numérique portuaire intégré et évolutif.

I-2 Situation actuelle et justification

Les dispositifs de contrôle d'accès en place aux portails P1 et P2 sont en état de vétusté avancée. Le contrôle des accès s'effectue actuellement de manière manuelle, sans traçabilité numérique, sans corrélation avec les données opérationnelles (missions, véhicules, cargaisons) et sans capacité d'alerte en temps réel. La SPAT est tenue de se doter d'un système automatisé et performant afin de se conformer aux recommandations des organismes nationaux et internationaux compétents (Organisation maritime internationale, US Coast Guard, APMF) et d'atteindre le niveau attendu d'un port sûr et performant au sens du Code ISPS. Au-delà de la conformité réglementaire, la réforme de P1 et P2 doit éviter l'écueil d'un excellent système de contrôle d'accès qui deviendrait demain un silo informatique. Le système acquis doit être architecturalement prêt à s'intégrer dans un écosystème plus large : système d'information portuaire, systèmes des acteurs institutionnels, terminaux, autres sites SPAT et système de supervision centralisé.

La mise en place d'un système de contrôle d'accès électronique intégré, couvrant à la fois les flux piétons et véhicules, et relié au poste de commandement central du port, est devenue incontournable.

I-3 Cadre réglementaire et pérennité

- **Code ISPS / SOLAS 1974 (amendé 2002)** : Exigences en matière de sûreté maritime et portuaires, notamment l'application rigoureuse des mesures adéquates concernant la gestion efficace et efficiente des accès aux zones réglementées.
- **Résolution IMO A.1154 (32)** : Directives pour la protection des ports et des installations portuaires.
- **ISO 9001: 2015** : Système de management de la qualité — applicable aux processus de contrôle et de maintenance.
- **IEC 60529** : Indice de protection des matériels électriques (indices IP) — IP65 minimum en extérieur, IP67 pour les lecteurs d'accès .
- **ISO/IEC 14443 & 15693** : Normes relatives aux cartes sans contact et aux lecteurs RFID.

- **ISO/IEC 19794** : Formats de données biométriques (empreinte digitale, image faciale).
- **Loi n° 2014-005 (17 juillet 2014)** : Relative à la lutte contre le terrorisme et la criminalité transnationale organisée à Madagascar — sécurisation des infrastructures critiques.
- **Loi n° 2014-006 : Relative à la lutte contre la cybercriminalité à Madagascar — fonde les exigences de cybersécurité du système.**
- **Loi n° 2014-038 (9 janvier 2015) : Relative à la protection des données à caractère personnel — institue la Commission Malgache de l'Informatique et des Libertés (CMIL). Encadre le traitement des données biométriques et des journaux d'accès du système.**
- **Pérennité** : Le système devra couvrir les besoins opérationnels du port sur un horizon de 15 à 20 ans, avec disponibilité des pièces de rechange et mises à jour logicielles garanties sur au moins 10 ans par le constructeur
- **Représentation locale**: Le titulaire devra disposer d'une représentation physique à Madagascar, apte à assurer le Service Après-Vente et les interventions techniques sur site dans les délais contractuels.
- **Niveaux de sûreté MARSEC (Code ISPS, partie A § B)** : Le système devra supporter l'adaptation dynamique des règles d'accès aux trois niveaux de sûreté maritime (MARSEC 1, 2 et 3), conformément aux exigences du Code ISPS.

II. OBJECTIFS DE LA MISSION

L'objectif principal est de doter le Port de Toamasina d'un Smart Gate — premier point d'accès intelligent de l'écosystème numérique SPAT 2.0 — aux portails P1 et P2. Ce système de contrôle et de gestion des accès doit être à la fois opérationnel dans un délai de vingt (20) semaines à compter de la date de versement de l'acompte à la commande, et conçu dès l'origine pour s'intégrer sans rupture dans les systèmes futurs de la SPAT et des autres sites SPAT.

- **Objectif 1 – Smart Gate : architecture évolutive et interopérable** : Concevoir et déployer P1 et P2 comme la première brique d'une architecture de contrôle d'accès mutualisée, extensible nativement aux autres sites SPAT, actuels et futurs, sans dépendance propriétaire, reposant sur des standards ouverts et une séparation claire entre couche physique (équipements), couche logique (contrôleurs, logiciel) et couche d'intégration (API).
- **Objectif 2 – Automatisation des accès piétons, motocyclettes et véhicules** : Remplacer les dispositifs manuels hors-service par des équipements industriels capables de gérer des flux intensifs, résistants à l'environnement salin du port, avec ouverture et fermeture automatiques commandées électroniquement. Inclure des barrières levantes motorisées pour les véhicules légers et les poids lourds, avec détection de présence et sécurité anti-écrasement.
- **Objectif 3 – Authentification sécurisée multi-facteurs** : Déployer des lecteurs d'accès biométriques combinant reconnaissance faciale et empreinte digitale, couplés à la lecture de badges sans contact, pour une authentification robuste de toutes les personnes accédant à l'enceinte portuaire.

- **Objectif 4 – Identification composite et contrôle de mission** : Permettre à terme d'associer, pour chaque passage, un ensemble cohérent de données : identité du chauffeur ou de l'agent, véhicule (plaque, type), entreprise mandataire, mission portuaire autorisée, et — pour les entrées marchandises — référence conteneur ou cargaison. L'accès ne devra plus reposer uniquement sur la validité d'un badge, mais sur la cohérence de l'ensemble de ces éléments. La Phase 1 (présent marché) posera les fondations logicielles et API nécessaires ; la Phase 2 activera les modules ANPR/LPR et OCR en s'appuyant sur l'infrastructure de vidéosurveillance existante du port.
- **Objectif 5 – Gestion centralisée, traçabilité et souveraineté des données** : Mettre en service un logiciel de gestion des accès avec licence perpétuelle, capable de gérer l'ensemble des identités actives du port, fonctionnel en mode hors-ligne, et intégré au poste de commandement central. La SPAT sera propriétaire exclusive de toutes les données collectées. L'hébergement, le chiffrement, les habilitations, les durées de conservation, les procédures de purge et d'audit devront être définis contractuellement. Toute exploitation des données par le fournisseur à des fins propres est strictement interdite.
- **Objectif 6 – Enrôlement, émission de badges et gestion des identités** : Déployer une station d'enrôlement biométrique et une imprimante à badge permettant la personnalisation et l'émission des titres d'accès pour l'ensemble du personnel, des prestataires et des visiteurs du port.
- **Objectif 7 – Formation et transfert de compétences** : Former 100 % du personnel désigné par la SPAT à l'utilisation et à la maintenance de premier niveau du système, dans un délai de deux (2) semaines suivant la réception provisoire.
- **Objectif 8 – API ouvertes et interopérabilité avec l'écosystème portuaire** : Exposer des API sécurisées, ouvertes et documentées (format OpenAPI/Swagger), consommables par toute application ou système tiers autorisé par la SPAT, sans recourir à un connecteur propriétaire du fournisseur. Ces API devront permettre l'intégration du système de contrôle d'accès avec l'ensemble des acteurs et outils numériques du port, actuels ou futurs, dans le cadre de l'architecture SPAT 2.0. La documentation complète de l'API devra être remise à la SPAT à la réception, avec les droits nécessaires à son exploitation autonome.
- **Objectif 9 – Compatibilité ANPR/LPR et OCR conteneurs (Phase 2 ready)** : Concevoir le système pour permettre, sans remplacement de l'architecture centrale, l'activation ultérieure de la reconnaissance automatique des plaques d'immatriculation (ANPR/LPR) et de l'OCR conteneurs, en exploitant l'infrastructure de vidéosurveillance existante aux portails. Le présent marché ne couvre pas l'acquisition de modules LPR/OCR, mais en pose les prérequis d'interface (API, schéma de données, connecteurs). L'identification composite chauffeur + véhicule + mission + cargaison pourra ainsi être activée en Phase 2 sans interruption du système.
- **Objectif 10 – Dashboard temps réel et KPIs opérationnels** : Fournir un tableau de bord temps réel exploitable depuis le poste de commandement, affichant les indicateurs opérationnels clés : Gate Processing Time (GPT) moyen et par voie, débit par heure par portail, temps d'attente moyen par voie, taux de traitement automatique vs. interventions manuelles, files d'attente en temps réel, taux de disponibilité système, et alertes actives. Ce dashboard devra exposer ses données via API afin de pouvoir être intégré à terme dans le système de supervision centralisé.

- **Objectif 11 – Extension native aux autres sites SPAT** : L'architecture logicielle et d'intégration retenue devra permettre nativement l'extension à d'autres points d'accès SPAT, actuels et futurs, sans refonte de l'architecture centrale. Le titulaire précisera dans son offre technique les conditions (licences, infrastructure, API) d'une telle extension.

III. SPÉCIFICATIONS TECHNIQUES DÉTAILLÉES

Toutes les spécifications ci-après sont ouvertes à la concurrence. Aucune marque ou modèle n'est imposé. Les soumissionnaires peuvent proposer tout équipement répondant aux exigences fonctionnelles et techniques définies, à charge pour eux de démontrer l'équivalence. L'environnement portuaire de Toamasina impose des contraintes spécifiques : atmosphère saline, humidité élevée, ensoleillement intense, poussière et risques de vandalisme. L'ensemble des équipements devra être dimensionné en conséquence.

1. Tourniquets industriels – contrôle des accès piétons

- **Type et hauteur** : Tourniquet à pleine hauteur (minimum 2,20 m) à passage bidirectionnel, de type industriel.
- **Résistance structurelle** : Structure en acier inoxydable de qualité industrielle, avec traitement anticorrosion certifié pour environnement salin marin.
- **Consommation électrique** : Ultra-basse consommation, inférieure à 5 W en veille.
- **Alimentation de secours** : Autonomie minimale de 2 heures sur batterie intégrée en cas de coupure secteur ; position de sécurité (fail-safe) configurable à l'ouverture ou à la fermeture.
- **Sens de passage** : Unidirectionnel ou bidirectionnel, paramétrable par commande logicielle sans intervention physique.
- **Protocole de communication** : Compatible avec le contrôleur d'accès via un protocole de communication sécurisé et chiffré, conforme aux standards reconnus du secteur ; le protocole retenu et son niveau de sécurité devront être documentés dans l'offre technique.
- **Débit** : Capacité minimale de 30 passages par minute et par voie en régime normal.
- **Quantité indicative** : Minimum 2 voies entrée + 2 voies sortie par portail (P1 et P2) — le soumissionnaire précisera le dimensionnement sur la base de son analyse.
- **Bouton d'activation d'urgence** : Commande pour un déverrouillage manuel pour les évacuations rapides des personnes en cas de danger ou de coupure de courant.

2. Barrières levantes automatiques – contrôle des accès véhicules

Les portails P1 et P2 accueillent un trafic mixte composé de véhicules légers, motorisés et de poids lourds (camions, semi-remorques, engins portuaires). Les équipements devront être dimensionnés en conséquence pour les deux catégories de véhicules.

- **Type** : Barrière levante motorisée à flèche, adaptée au trafic intensif en milieu portuaire, compatible avec le passage de poids lourds et de semi-remorques.
- **Longueur de flèche** : Dimensionnée selon la largeur de chaque voie de passage, incluant les voies poids lourds ; lestage ou équilibrage automatique inclus.

- **Motorisation** : Puissance adaptée aux cycles intensifs générés par le trafic poids lourds ; protection thermique intégrée et détection d'obstacle anti-écrasement obligatoire.
- **Vitesse d'ouverture / fermeture** : Inférieure à 3 secondes pour assurer la fluidité du trafic véhicules légers et poids lourds.
- **Résistance environnementale** : Boîtier moteur en protection IP54 minimum ; traitement anticorrosion pour environnement salin.
- **Alimentation de secours** : Déverrouillage manuel sécurisé ; option d'alimentation sur batterie de secours avec une autonomie minimale de 2 heures.
- **Pilotage** : Commandable par le contrôleur d'accès (sortie relais) et par télécommande ou bouton-poussoir de proximité.
- **Détection de présence** : Boucles inductives ou capteurs au sol sur les voies poids lourds, empêchant toute fermeture intempestive sur un véhicule en cours de passage.
- **Quantité indicative** : Minimum 2 barrières entrée (véhicules légers et poids lourds) + 2 barrières sortie par portail, soit 8 unités au minimum — le soumissionnaire précisera si des voies dédiées poids lourds nécessitent des équipements distincts ou si une voie mixte peut être retenue.

3. Lecteurs d'accès biométriques

- **Technologies de lecture** : Multi-technologie obligatoire : reconnaissance faciale haute précision et empreinte digitale, avec lecture de badges sans contact (conforme ISO/IEC 14443 et ISO/IEC 15693).
- **Protection** : Indice de protection IP67 minimum (étanchéité à l'immersion) ; résistance IK08 minimum contre les chocs et le vandalisme.
- **Temps de vérification** : Inférieur à 1 seconde pour la reconnaissance faciale et l'empreinte.
- **Base de données locale** : Capacité de stockage local couvrant l'ensemble des identités actives disposant de droits d'accès sur le portail, pour un fonctionnement autonome hors-ligne sans dégradation du temps de vérification. Le soumissionnaire précisera la capacité réelle proposée et sa justification au regard des flux portuaires et de l'évolution prévisible du nombre de badges actifs sur P1/P2 ; une capacité ne permettant pas d'héberger localement la totalité des identités actives sera considérée comme non conforme.
- **Anti-fraude** : Détection de faux visage (anti-spoofing), détection de faux doigt, détection de présence à proximité immédiate.
- **Affichage** : Retour visuel à l'utilisateur (écran couleur ou indicateurs LED).
- **Connectivité** : Interface réseau TCP/IP ; les communications entre lecteurs et contrôleur devront être chiffrées par un protocole sécurisé conforme aux standards du secteur, documenté dans l'offre.
- **Alimentation** : Alimentation par le réseau ou alimentation basse tension dédiée, avec protection contre les surtensions.

- **Implantation sur voies poids lourds** : Sur les voies accueillant des poids lourds et semi-remorques, les lecteurs devront être montés sur colonne ou potelet à hauteur adaptée à la cabine de conduite (entre 1,5 m et 2,2 m selon configuration) ; le soumissionnaire précisera le dispositif retenu pour chaque voie dans son plan d'implantation.
- **Traçabilité des sorties** : Des lecteurs d'accès devront être installés sur toutes les voies de sortie — piétons et véhicules, y compris poids lourds — afin d'enregistrer chaque sortie avec le même niveau de détail que les entrées (identité, horodatage, point de passage) ; aucune sortie ne doit pouvoir s'effectuer sans enregistrement dans le système.
- **Quantité indicative** : Sur la base de 2 voies piétons entrée + 2 voies piétons sortie + 1 voie véhicules légers entrée + 1 voie véhicules légers sortie + 1 voie poids lourds entrée + 1 voie poids lourds sortie par portail, le nombre minimum de lecteurs est de 8 unités par portail, soit 16 unités pour P1 et P2 — le soumissionnaire affinera ce chiffre dans son plan d'implantation sur la base des configurations réelles des portails.

4. Contrôleur d'accès (unité centrale de gestion)

- **Capacité de gestion** : Au minimum 10 portes câblées par unité, avec possibilité d'extension.
- **Base de données** : Gestion en cache local de l'ensemble des identités actives disposant de droits d'accès sur le site, synchronisées depuis la base centrale, avec historique consultable ; le cache local est distinct de la base totale d'identités enrôlées gérée par le logiciel (§ 5) ; architecture extensible permettant la couverture multi-sites.
- **Mode hors-ligne** : Fonctionnement autonome complet en cas de perte de connexion au serveur central ; application des règles d'accès en local, en temps réel.
- **Journal d'événements local** : Capacité minimale de 500 000 événements horodatés (passages, refus, alarmes), soit au moins 30 jours d'autonomie au débit de pointe, sans écrasement cyclique ; synchronisation automatique et intégrale vers le serveur central au rétablissement de la liaison. Les offres proposant une capacité de 2 000 000 d'événements ou plus seront valorisées.
- **Sécurité** : Logique programmable embarquée ; chiffrement des communications ; politiques d'accès appliquées indépendamment du serveur.
- **Alarmes** : Surveillance et remontée des alarmes anti-intrusion vers le poste de commandement (Control Room).
- **Connectivité réseau** : Double interface réseau pour redondance et continuité de service
- **Intégration** : Prise en charge de l'intégration directe avec les systèmes de gestion technique du bâtiment existants.
- **Fiabilité** : Fonctionnement continu 24h/24, 7j/7 ; MTBF $\geq$ 50 000 heures.
- **Anti-passback** : Fonction anti-passback activable par zone et par portail : empêche la réutilisation d'un badge sans sortie préalablement enregistrée ; paramétrable en mode strict ou tolérant selon le profil utilisateur.
- **Adaptation aux niveaux de sûreté (MARSEC)** : Prise en charge des trois niveaux de sûreté maritime MARSEC 1, 2 et 3 : modification automatique des règles d'accès

(facteurs d'authentification requis, zones autorisées, délais) sur déclenchement par commande opérateur depuis le poste de commandement.

- **Révocation instantanée** : Propagation immédiate de toute révocation ou suspension de badge sur l'ensemble des contrôleurs et points d'accès, y compris mise à jour forcée des caches locaux en mode hors-ligne ; délai de propagation maximum de trente (30) secondes sur l'ensemble du réseau.

5. Logiciel de gestion des accès

— Fondamentaux

- **Type de licence** : Licence perpétuelle (à vie), sans abonnement annuel obligatoire pour les fonctionnalités de base.
- **Capacité** : Gestion d'au minimum 1 000 000 d'identités enregistrées, couvrant l'ensemble des catégories d'usagers du port : employés permanents, conducteurs de poids lourds, chauffeurs de véhicules légers, visiteurs, prestataires et sous-traitants, ainsi que d'un référentiel des véhicules autorisés associés à ces identités (cf. Gestion des véhicules autorisés). Ce dimensionnement est prévu pour couvrir un horizon de 15 à 20 ans d'exploitation, en intégrant l'ensemble des catégories d'usagers susceptibles d'être enregistrés ainsi que la croissance prévisible des flux portuaires ; architecture scalable et administration multi-sites.

— Fonctionnalités

- **Fonctionnalités** : Gestion des droits par profil et plages horaires ; journaux d'audit complets, infalsifiables et conservés sur une durée minimale de douze (12) mois conformément aux exigences du Code ISPS ; traçabilité complète des entrées et des sorties pour chaque personne et chaque véhicule, avec horodatage et identité ; rapports de présence, de trafic et de temps de séjour dans l'enceinte ; gestion des alarmes et des incidents.
- **Interface** : Disponible en français ou en anglais ; documentation technique complète en français.
- **Gestion des véhicules autorisés** : Module de gestion d'un référentiel des véhicules habilités à entrer dans l'enceinte : immatriculation, type (véhicule léger, poids lourd, semi-remorque, motocyclette), entreprise rattachée, période de validité, zones autorisées. Chaque véhicule pourra être associé à une ou plusieurs identités (chauffeurs habilités) et à une mission portuaire. Le contrôle de cohérence chauffeur / véhicule / mission devra être activable par règle, en préparation de l'identification composite et de l'intégration ANPR/LPR (Phase 2). Les véhicules autorisés pourront être créés ou mis à jour depuis un référentiel externe de la SPAT ou de l'écosystème portuaire via l'API (cf. Synchronisation des identités et des véhicules). Suspension et révocation d'un véhicule avec propagation immédiate à l'ensemble des points d'accès.
- **Gestion des visiteurs et prestataires** : Module dédié à la gestion des accès temporaires : pré-enregistrement des visiteurs, émission de badges à durée d'expiration automatique, règles d'escort paramétrables par profil, traçabilité complète des accès et révocation automatique en fin de visite.

— Fiabilité et pérennité

- **Dashboard opérationnel temps réel** : Le logiciel devra inclure un tableau de bord exploitable depuis le poste de commandement (Control Room) affichant en temps réel : état de chaque voie (ouverte/fermée/alarme), flux d'accès en cours, alertes actives, Gate Processing Time par voie, temps d'attente moyen par voie, débit cumulé par heure et occupation des zones. Les données du dashboard devront être accessibles par un système tiers (système de supervision centralisé) selon l'une des deux modalités suivantes, au choix du soumissionnaire : (a) API REST documentée au format OpenAPI/Swagger, stable et consommable sans développement spécifique imposé par le fournisseur ; ou (b) accès direct à la base de données du logiciel, avec schéma de données documenté et engagement contractuel de stabilité du schéma sur la durée de la garantie. Dans les deux cas, l'intégration ne devra pas nécessiter l'intervention payante du fournisseur. La documentation complète (schéma de base de données annoté ou spécification API au format OpenAPI/Swagger) devra être remise physiquement à la SPAT au moment de la réception provisoire (SAT), sous forme de fichier exploitable.
- **Haute disponibilité** : Sauvegarde automatique des bases de données ; procédures documentées de reprise après sinistre.
- **Évolutivité** : Architecture modulaire permettant l'ajout ultérieur de nouveaux modules (interphonie, contrôle de flux, etc.) sans remplacement du cœur du système.
- **Réversibilité des données** : L'ensemble des données du système (identités, journaux d'accès, configurations, règles d'accès) devra être exportable à tout moment dans un format ouvert et documenté, permettant à la SPAT de migrer vers un autre système sans perte d'historique ni dépendance au titulaire.

— Intégration et interopérabilité

- **Interopérabilité via API** : Le système devra exposer des API sécurisées, ouvertes et documentées au format OpenAPI/Swagger, consommables par toute application ou système tiers autorisé par la SPAT, sans recourir à un connecteur propriétaire. Ces API devront couvrir au minimum les cinq fonctions ci-dessous et permettre l'intégration avec l'ensemble des acteurs et outils numériques de l'écosystème portuaire, dans le cadre de l'architecture cible SPAT 2.0.
 - **Événements et alarmes** : publication en temps réel des événements du système (accès accordé/refusé, alarme, anomalie détectée) à destination de systèmes abonnés.
 - **Consultation d'état** : interrogation de l'état courant des équipements (portes, barrières, tourniquets) par des systèmes tiers autorisés.
 - **Commandes à distance** : réception et exécution de commandes d'ouverture, de fermeture ou de dérogation émises par la passerelle d'intégration.
 - **Synchronisation des identités et des véhicules** : échange bidirectionnel des données de titulaires et de véhicules autorisés (création, modification, révocation de badges ou d'autorisations véhicules) avec les systèmes RH, de gestion des visiteurs, de gestion de flotte ou tout autre référentiel de la SPAT et de l'écosystème portuaire.
 - **Sécurité des échanges** : authentification des appels API par jeton (OAuth 2.0 ou équivalent) ou certificat ; toutes les communications devront être chiffrées (TLS 1.2 minimum) ; la documentation technique complète de l'API (format

OpenAPI/Swagger) devra être remise à la SPAT à la réception avec les clés et secrets associés.

- **Interface ANPR/LPR et OCR (Phase 2 ready)** : Le système devra exposer via API un point d'intégration documenté permettant l'alimentation en temps réel par un module ANPR/LPR ou OCR externe. Ce point d'intégration recevra les données de reconnaissance (plaque d'immatriculation, numéro de conteneur, timestamp, caméra source) et les associera à l'événement d'accès correspondant. Aucun équipement ANPR/LPR n'est requis dans le cadre du présent marché ; la conformité à cette exigence sera vérifiée par test d'interface simulé lors du SAT.
- **Compatibilité avec le système de vidéosurveillance existant (CCTV)** : Le système de contrôle d'accès devra être en mesure de s'interfacer avec le VMS en place à la SPAT, indépendamment de sa marque ou plateforme, en assurant au minimum les trois fonctions ci-dessous.
 - **Déclenchement caméra sur événement** : tout événement d'accès (passage autorisé, accès refusé, alarme) doit pouvoir déclencher automatiquement une action sur la caméra associée au point d'accès concerné (enregistrement, capture, alerte opérateur).
 - **Corrélation événements / images** : les journaux d'accès du système doivent pouvoir être liés aux séquences vidéo correspondantes pour consultation en salle de commandement ou en mode forensique.
 - **Documentation d'intégration** : le soumissionnaire devra préciser dans son offre technique les protocoles et mécanismes d'intégration proposés avec les systèmes VMS du marché, ainsi que les éventuelles conditions ou prérequis côté CCTV existants.

6. Station d'enrôlement et imprimante à badge

- **Station biométrique** : Dispositif de capture d'empreintes digitales et de photographie faciale pour l'enrôlement des utilisateurs.
- **Imprimante à badge** : Imprimante à badge professionnelle pour l'impression de badges personnalisés comportant données biométriques et visuelles.
- **Logiciel d'enrôlement** : Solution intégrée permettant la personnalisation et l'encodage des badges sans contact.
- **Capacité de production** : Minimum 200 badges par heure en régime de crête.
- **Format de badge** : ISO CR-80 standard (85,6 × 54 mm), épaisseur 0,76 mm (Carte DESFIRE EV3 NXP capacité 4ko ou 8ko).
- **Lot initial de cartes vierges** : Fourniture d'un lot initial d'au minimum 5 000 cartes RFID vierges format ISO CR-80, compatibles avec les lecteurs et l'imprimante à badge proposés, inclus dans l'offre de base.

7. Infrastructure, câblage et alimentation

- **Câblage** : Câbles blindés résistants aux interférences électromagnétiques, sous conduits de protection rigides adaptés dans les zones de passage véhicules.

- **Alimentation sans interruption** : Onduleur (UPS) dimensionné pour couvrir l'ensemble des équipements actifs (contrôleurs, lecteurs, serveur) avec une autonomie minimale de 4 heures (porté à 8 heures recommandées pour résistance aux situations cycloniques). En cas de coupure prolongée, le système devra basculer automatiquement en mode dégradé sécurisé : contrôleurs et lecteurs autonomes, enregistrement local, synchronisation différée à la remise en ligne.
- **Coffrets électriques** : Protection IP65 minimum pour tous les équipements d'alimentation et de contrôle installés en extérieur.
- **Serveur dédié (fourni par le titulaire)** : Le titulaire est responsable de la fourniture, du dimensionnement, de l'installation et de la mise en service d'un serveur dédié au système Smart Gate P1-P2. Ce serveur est intégré dans l'offre financière et devient propriété de la SPAT à la réception provisoire.
- **Spécifications matérielles minimales** : Processeur ≥ 8 cœurs physiques / 16 threads (architecture x86-64) ; RAM ≥ 32 Go ECC ; Stockage $\geq 2 \times 2$ To SSD NVMe en RAID 1 (miroir) + 1×4 To HDD pour archivage journaux ; Carte réseau $\geq 2 \times 1$ Gbps (agrégation/failover) ; Alimentation redondante (double PSU) ; Rack 19", profondeur ≤ 700 mm.
- **Logiciels de base inclus** : Système d'exploitation serveur sous licence permanente (ou open-source à justifier) ; Système de gestion de base de données (SGBD) adapté aux volumes et aux exigences de disponibilité ; Logiciel de sauvegarde automatisée intégré.
- **Redondance et disponibilité** : Architecture garantissant une disponibilité système $\geq 99,5$ % (hors maintenance planifiée) ; mécanisme de basculement automatique (failover) en cas de défaillance d'un composant critique ; politique de sauvegarde quotidienne avec rétention minimale 30 jours, hebdomadaire 6 mois.
- **Installation sur site SPAT** : Le serveur est physiquement installé dans les locaux de la SPAT (on-premise), dans une baie sécurisée ou salle serveur désignée. Aucune donnée biométrique ou journal d'accès ne transite vers un hébergement cloud externe.
- **Transfert de propriété et souveraineté** : À la réception provisoire (SAT), le titulaire remet à la SPAT l'intégralité des accès administrateurs (root/admin OS, SGBD, logiciel applicatif), des licences, des clés de chiffrement et de la documentation d'administration. La SPAT dispose d'un contrôle total et exclusif sur le serveur et les données qu'il héberge.

8. Cybersécurité et durcissement du système

- **Durcissement (hardening)** : Le système livré (serveur, contrôleurs, logiciel) devra être configuré selon les bonnes pratiques de durcissement reconnues : suppression des comptes et services inutiles, désactivation des ports réseau non utilisés, séparation des privilèges administrateurs — un rapport de configuration de sécurité sera remis à la SPAT à la réception.
- **Gestion des mises à jour et correctifs** : Le titulaire s'engage à notifier la SPAT de toute mise à jour critique de sécurité dans un délai de quinze (15) jours calendaires après publication par l'éditeur ; les correctifs devront être applicables sans interruption de service ou dans une fenêtre de maintenance planifiée et acceptée par la SPAT.

- **Segmentation réseau et résilience télécom** : Le système de contrôle d'accès devra être déployé sur un segment réseau dédié, isolé du réseau bureautique général de la SPAT. En cas de perte du lien réseau principal (fibre ou radio), chaque contrôleur devra continuer à fonctionner de manière autonome : application des règles d'accès locales, enregistrement des passages, gestion des alarmes. La synchronisation avec le serveur central s'effectuera automatiquement à la remise en ligne, sans perte de données. Toute communication inter-segments devra transiter par des points de contrôle documentés.
- **Pare-feu et détection d'intrusion** : Conformément aux exigences du Code ISPS relatives à la protection des systèmes d'information des installations portuaires critiques, le segment réseau dédié au contrôle d'accès devra être protégé par un pare-feu matériel ou logiciel configuré en liste blanche (whitelist), n'autorisant que les flux strictement nécessaires au fonctionnement du système. Un mécanisme de détection d'intrusion (IDS/NIDS) devra être mis en place sur ce segment et configuré pour générer des alertes vers le poste de commandement en cas de trafic anormal ou de tentative d'accès non autorisée. Les règles de filtrage et les logs d'alerte devront être accessibles et auditable par la SPAT.
- **Authentification administrative** : Authentification renforcée obligatoire pour tous les comptes administrateurs du logiciel et du serveur ; journalisation exhaustive de toutes les actions administratives ; politique de gestion des mots de passe documentée et remise à la SPAT.
- **Analyse de vulnérabilités** : Le titulaire remettra à la réception un rapport d'analyse de vulnérabilités du système livré, avec plan de remédiation pour toute vulnérabilité identifiée de niveau critique ou élevé.
- **Souveraineté et gouvernance des données biométriques** : Les données biométriques (gabarits d'empreintes, données faciales) et les journaux d'accès sont la propriété exclusive de la SPAT. Le titulaire ne pourra en aucun cas les exploiter, les transmettre, les stocker hors site ou les utiliser à des fins propres. L'hébergement devra être exclusivement local (serveur SPAT on-premise). Les données biométriques devront être chiffrées au repos (AES-256 minimum) et en transit. Le titulaire remettra à la SPAT : (i) la politique de gestion des accès aux données biométriques, (ii) les procédures de purge sécurisée à la fin de contrat, (iii) la liste exhaustive des habilitations d'accès aux données. Toute extraction de données biométriques sans autorisation écrite préalable de la SPAT constitue une faute grave.
- **Conformité à la Loi n° 2014-038 (protection des données à caractère personnel)** : Le logiciel devra intégrer un registre des traitements de données personnelles, un paramétrage des durées de conservation par catégorie de données, une purge automatique à échéance, et la journalisation de toute consultation de données personnelles. Il devra permettre l'extraction, la rectification et l'effacement des données d'une personne déterminée sur demande. Le titulaire remettra à la SPAT la documentation nécessaire à l'accomplissement de ses formalités auprès de la Commission Malgache de l'Informatique et des Libertés (CMIL).

IV. OUTILS, SUPPORTS ET TRAÇABILITÉ EXIGÉS

- **Documentation technique complète** : Plans d'implantation, schémas électriques, manuels d'installation, manuels d'utilisation et de maintenance — en français, pour chaque composant du système.
- **Fiches techniques constructeur** : Datasheets de chaque équipement fourni, en français ou en anglais avec traduction des éléments critiques de sécurité.
- **Journal de chantier** : Carnet de bord tenu à jour quotidiennement pendant la phase d'installation, remis intégralement à la SPAT à la réception.
- **Protocole FAT** : Document de recette en usine (Factory Acceptance Test) soumis à la SPAT pour validation au minimum quinze (15) jours avant toute expédition.
- **Protocole SAT** : Document de recette sur site (Site Acceptance Test) cosigné par le titulaire et la SPAT après mise en service complète.
- **Lot de pièces de rechange** : Lot couvrant au minimum les 3 premières années de maintenance : alimentations, fusibles, lecteurs de remplacement, relais et câbles de raccordement.
- **Outillage spécialisé** : Kit d'outillage spécifique fourni si la maintenance de premier niveau requiert des outils indisponibles sur le marché local Malgache.
- **Accès au support constructeur** : Portail de support en ligne documenté ou hotline technique, avec engagement contractuel de temps de réponse.

Critères d'acceptation FAT et SAT — seuils contractuels

- **Reconnaissance biométrique** : Taux de fausse acceptation (FAR) inférieur à 0,001 % et taux de faux rejet (FRR) inférieur à 0,1 %, mesurés sur un échantillon minimum de 500 passages lors du SAT.
- **Temps de vérification** : Temps de passage biométrique inférieur à 1 seconde mesuré sur la totalité des passages de test lors du SAT — tout dépassement systématique constitue un motif de refus de réception.
- **Stabilité en test continu** : Aucune interruption de service non planifiée durant les 48 heures de test continu précédant la signature du PV SAT.
- **Fonctionnement hors-ligne** : Démonstration obligatoire du fonctionnement autonome complet (accès, journalisation, alarmes) lors d'une simulation de coupure réseau d'une durée minimale de quatre (4) heures lors du SAT.
- **Test de révocation** : Propagation d'une révocation de badge vérifiée sur tous les points d'accès en moins de trente (30) secondes lors du SAT.
- **Test de niveau de sûreté (MARSEC)** : Démonstration du passage entre les trois niveaux MARSEC (1 → 2 → 3 → 1) avec adaptation automatique des règles d'accès, mesurée et consignée dans le PV SAT.

V. LIVRABLES ATTENDUS

1. **Dossier d'homologation et certificats de conformité** : documents prouvant la conformité aux normes citées en Section I-3 (ISPS, IEC 60529, ISO/IEC 14443, ISO/IEC 19794, etc.), émis par des organismes certificateurs reconnus.
2. **Certificat d'engagement du représentant local** : document officiel attestant de la présence physique à Madagascar d'un partenaire ou représentant du titulaire, avec coordonnées et engagement contractuel de délai d'intervention.
3. **Certificat de garantie constructeur** : garantie d'au minimum 3 ans sur l'ensemble des équipements fournis, couvrant pièces et main-d'œuvre - les offres proposant 4 ou 5 ans seront valorisées .
4. **Livraison physique et installation sur site** : livraison au Port de Toamasina, déchargement, mise en place, câblage, paramétrage et mise en service complets de l'ensemble du système.
5. **Procès-verbal de réception FAT** : PV cosigné par le titulaire et la SPAT attestant de la conformité des équipements avant expédition.
6. **Procès-verbal de réception SAT** : PV cosigné sur site après mise en service, attestant que le système fonctionne conformément aux présentes spécifications dans les conditions réelles du port .
7. **Manuel de maintenance simplifié** : guide pratique en français destiné aux équipes techniques de la SPAT : maintenance de premier niveau, diagnostic des pannes courantes, remplacement des consommables.
8. **Attestations de formation certifiées** : certificats remis à chaque agent formé, signés par le titulaire et la SPAT, couvrant 100 % du personnel désigné : opérateurs, agents de sûreté portuaire, techniciens IT.
9. **Contrat de maintenance préventive et corrective** : proposition de contrat SAV post-garantie avec SLA définis : délais d'intervention, taux de disponibilité garanti, délais de livraison de pièces de rechange.
10. **Rapport de configuration système** : documentation exhaustive de la configuration déployée (paramètres logiciels, plan réseau, règles d'accès, liste des utilisateurs enrôlés) — remise en version papier et numérique.
11. **Plan de réversibilité et portabilité des données** : document décrivant les formats d'export de l'ensemble des données du système (identités, journaux, configurations) et la procédure de migration vers un système tiers ; un export de démonstration sera produit et remis à la SPAT lors de la réception provisoire.
12. **Plan de continuité d'activité (PCA)** : document décrivant les procédures de reprise en cas de défaillance majeure du serveur central : procédures de sauvegarde et restauration, basculement en mode autonome distribué, délais de reprise cibles — les procédures devront être testées et validées lors du SAT.

VI. CHRONOGRAMME ET DÉLAIS DE MISE EN ŒUVRE

Le délai global de réalisation est fixé à vingt (20) semaines — soit cinq (5) mois — à compter de la date de versement de l'acompte à la commande. Le titulaire soumettra à la SPAT, au plus tard à S+1, un planning détaillé qui, après validation par la SPAT à S+2, constituera une pièce contractuelle du marché. Ce planning précisera notamment les délais de fabrication, les modalités d'expédition et le séquençage de l'installation sur site.

Jalon / Livrable	Délai	Responsable
Remise du planning détaillé et des spécifications d'implantation	S+1	Titulaire
Validation du planning détaillé par la SPAT	S+2	SPAT
Premier rapport d'avancement fabrication / approvisionnement	S+4	Titulaire
Rapport d'avancement fabrication et validation des spécifications finales	S+10	Titulaire + SPAT
Factory Acceptance Test (FAT) — inspection avant expédition	☐ S+14	Titulaire + SPAT
Expédition et transport vers Toamasina	S+15	Titulaire
Réception physique des équipements au Port de Toamasina	S+17	Titulaire + SPAT
Installation, câblage et mise en service sur site	S+17 à S+18	Titulaire
Site Acceptance Test (SAT) et PV de réception provisoire	☐ S+18	Titulaire + SPAT
Formation des équipes SPAT	☐ S+19	Titulaire
Contractualisation SAV et transfert formel de propriété	☐ S+20	Titulaire + SPAT

☐ Jalons contractuels : leur non-respect déclenche les pénalités de retard. Les jalons sans ce symbole sont des points de suivi informatifs.

Les délais ci-dessus sont contractuellement impératifs. Tout retard non-justifié et non accepté par la SPAT entraînera l'application des pénalités de retard prévues au contrat.

À titre indicatif, les pénalités de retard applicables seront de l'ordre de 0,5 % du montant total du marché par semaine de retard constatée, plafonnées à 10 % du montant total du marché. Au-delà de ce plafond, la SPAT se réserve le droit de résilier le marché aux torts exclusifs du titulaire, sans préjudice des dommages et intérêts pouvant être réclamés. Les montants définitifs seront fixés dans les Conditions Particulières du marché.

VII. ALIGNEMENT AVEC LES CRITÈRES D'ÉVALUATION DU DAO

L'évaluation des offres sera conduite sur la base des critères pondérés ci-dessous. La grille intègre des critères structurants de SPAT 2.0 — interopérabilité, cybersécurité et souveraineté des données — permettant de différencier les offres sur leur capacité à s'inscrire dans l'écosystème Smart Port, au-delà de la seule conformité technique immédiate. La SPAT se réserve le droit d'ajuster les pondérations lors de la finalisation du DAO, dans le respect des règles de passation des marchés applicables.

Critère d'évaluation	Pondération	Éléments d'appréciation
Conformité technique aux spécifications	25 %	Respect point par point de la Section III (équipements, biométrie, modes opérationnels, résilience, FAT/SAT) ; démonstration de l'équivalence pour tout composant proposé en substitution
Interopérabilité et Smart Port readiness	15 %	Qualité et maturité de l'API exposée (conformité OpenAPI/Swagger, couverture fonctionnelle, documentation) ; interface ANPR/LPR Phase 2 ready démontrée lors du SAT ; capacité d'intégration avec l'écosystème portuaire documentée ; absence de verrouillage propriétaire ; extensibilité multi-sites
Cybersécurité et souveraineté des données	10 %	Hébergement on-premise exclusif ; chiffrement des données biométriques (AES-256 min.) ; politique d'habilitation, de conservation et de purge documentée ; rapport de durcissement ; interdiction d'exploitation des données par le fournisseur contractuellement garantie
Qualité et robustesse de la solution	10 %	Références de déploiements similaires en environnement portuaire ou industriel ; certifications constructeur (ISO 9001, IEC 60529, etc.) ; résilience

		cyclonique/électrique/télécom démontrée
Coût Total de Possession sur 10 ans (TCO)	20 %	Prix d'acquisition + maintenance préventive + pièces de rechange + formation continue + coût de la licence logicielle sur 10 ans + coût d'extension éventuelle aux autres sites SPAT
Présence locale et capacité SAV à Madagascar	10 %	Représentation physique à Madagascar (adresse vérifiable) ; délai d'intervention garanti à Toamasina ; stock local de pièces de rechange
Délai global de réalisation	5 %	Respect du délai contractuel de 20 semaines ; qualité et crédibilité du planning détaillé
Durée de garantie proposée	3 %	Note minimale pour 3 ans ; bonification progressive jusqu'à 5 ans
Qualité du plan de formation	2 %	Couverture à 100 % du personnel désigné ; qualité des supports pédagogiques ; remise d'attestations certifiées

Niveaux de service (SLA) exigibles

- **Prise en charge du diagnostic** : Délai maximum de 4 heures ouvrables après signalement d'un incident critique.
- **Intervention sur site à Toamasina** : Délai maximum de 24 heures pour tout incident bloquant affectant P1 ou P2.
- **Disponibilité contractuelle du système** : Minimum 99,5 % sur base annuelle, hors fenêtres de maintenance préventive planifiées et acceptées par la SPAT.
- **Livraison de pièces de rechange** : Maximum 15 jours ouvrables pour les pièces non stockées localement.
- **Disponibilité des pièces garantie** : Minimum 10 ans à compter de la réception provisoire — engagement écrit du constructeur exigé.

Le présent Termes de Référence constitue le document technique de référence pour l'élaboration et l'évaluation des offres dans le cadre du Dossier d'Appel d'Offres relatif à la mise en place du Smart Gate P1-P2 — première brique du Smart Port Toamasina / SPAT 2.0. Il

engage les soumissionnaires à proposer non pas un simple système de contrôle d'accès fermé, mais une solution ouverte, souveraine et extensible, conçue pour s'intégrer dans l'écosystème numérique portuaire de demain. Toute demande de clarification devra être adressée par écrit à la SPAT dans les délais prévus par le DAO.

NB : La demande des dossiers DAO est subordonnée à l'acquittement de droit d'ariary un million(1000 000) ou son équivalent en monnaie étrangère

, à verser au compte BRED de la SPAT n°00008 0049 02001000034 87

MG46/0000/8004/9002/0010/0003/487 BFAVMGMGXXX

IBAN

BIC SWIFT