Cahier des charges pour appels d’offres   
  
MOOV Multi-Tenant

2021-03-23 | version 1.0

Ce document est destiné à apporter une aide aux professionnels qui préparent des cahiers des charges concernant des projets, des demandes d'informations (DI) ou de propositions (DP), et des appels d'offres pour des systèmes de gestion des stationnements pour les parkings partagés.

Les charges sont classées par thème.

Nedap se réserve le droit de modifier ce document sans préavis écrit. Le fournisseur des produits spécifiés peut être contacté à l'adresse suivante :

Nedap Identification Systems

P: +31 544 471 111

E: info@nedapidentification.com

<http://www.nedapidentification.com>

**Sommaire**

[1 Description du fonctionnement 4](#_Toc67401102)

[2 Contrôleurs 5](#_Toc67401103)

[3 Système de gestion central 6](#_Toc67401104)

[4 Création et gestion de groupes et de la capacité de stationnement 7](#_Toc67401105)

[5 Vue d’ensemble et commande à distance 8](#_Toc67401106)

[6 Journal de bord des évènements 9](#_Toc67401107)

[7 Gestion des droits d’accès 10](#_Toc67401108)

[8 Evènements et fenêtres de temps 11](#_Toc67401109)

[9 Accessibilité des services d’urgence et d’assistance 12](#_Toc67401110)

[Avertissement 13](#_Toc67401111)

[Document revisies 13](#_Toc67401113)

# Description du fonctionnement

Le système vise à être déployé pour permettre l'accès sélectif des véhicules à un parking partagé sur la base d'une capacité prédéfinie pour chaque groupe d'utilisateurs.

Dans le cadre de cette application, l'accès des véhicules doit être régulé au moyen de systèmes d'accès, matérialisés par la présence d'une ou plusieurs barrières qui peuvent être actionnées automatiquement ou manuellement, et à distance depuis n'importe quel endroit.

Les systèmes d'accès doivent pouvoir fournir un accès automatique aux véhicules bénéficiant de droits d'accès valides, en ouvrant automatiquement la ou les barrières après identification et vérification des moyens d'accès.

Avant d'accorder l'accès, le système doit pouvoir vérifier à quel groupe de stationnement le véhicule appartient ainsi que la capacité disponible pour ce groupe de stationnement.

Si le véhicule identifié se révèle appartenir à un groupe de stationnement pour lequel la capacité prédéfinie a déjà été atteinte, l'accès automatique ne doit pas être accordé à ce véhicule.

Le système doit prendre en charge tous les moyens d'accès courants, tels que la reconnaissance des plaques d'immatriculation, les cartes d'accès, les transpondeurs, les QR codes, Bluetooth et NFC.

En plus du contrôle local, tous les systèmes d'accès inclus dans le projet doivent être contrôlés au sein d'un système de gestion central qui détermine et met en œuvre la politique d'accès souhaitée en définissant des fenêtres de temps, en enregistrant les moyens d'accès autorisés et en activant à distance le cas échéant le fonctionnement des barrières.

Le système de gestion central doit être proposé comme une solution de Software-as-a-Service (SaaS) afin que les utilisateurs puissent accéder au panneau de commande et à la gestion des droits d'accès à tout moment et de n'importe quel endroit via Internet.

Les moyens d'accès autorisés et les fenêtres de temps doivent en permanence être synchronisés par le système de gestion central avec un stockage local au niveau des systèmes d'accès concernés, afin que le contrôle d'accès reste opérationnel lorsqu'une connexion Internet est temporairement impossible.

Pour ce faire, les systèmes d'accès doivent être équipés de contrôleurs spécialement conçus pour l'accès des véhicules, appelés « contrôleurs de gestion des véhicules ».

# Contrôleurs

Le type de contrôleur de gestion de véhicule doit avoir les fonctionnalités et propriétés suivantes :

* Le stockage des données au niveau local - y compris les moyens d'accès valides, les fenêtres de temps, le registre des événements - et la synchronisation automatique de ces derniers avec le système de gestion central ;
* Connecter et contrôler au moins deux barrières ;
* Connexion d'au moins 4 lecteurs d'identification reposant sur plusieurs types d'identification (c'est-à-dire badges, étiquettes, reconnaissance de plaque d'immatriculation, biométrie, téléphones portables) ;
* Connexion des caméras de plaque d'immatriculation via IP ;
* Connexion des feux de signalisation LED jusqu'à 24V 2x2 (rouge / vert) ;
* Surveiller la vitesse de déplacement et l’orientation correcte de la barrière ;
* Fonctionnement certifié à une température allant de -30°C à +60°C ;
* Indice de protection IP22 ou plus.
* Possibilité de connecter à une enseigne Alenco.

# Système de gestion central

Toutes les informations concernant l'activité d'accès aux systèmes d'accès doivent être recueillies et intégrées à un serveur central hébergé dans le Cloud.

Le fournisseur doit être en mesure de présenter à la fois le journal de bord des événements pour chaque accès, ainsi que le contrôle manuel des systèmes d'accès et la saisie et la gestion des droits d'accès, dans une seule application web.

Le système de gestion central doit être accessible depuis n'importe quel navigateur Web actuel prenant en charge Java.

Le système de gestion central doit utiliser les protocoles industriels standards (tels que REST ou REST Hooks) pour permettre l'intégration à des systèmes tiers.

La documentation décrivant les REST Hooks existants doit être disponible et accessible depuis le système de gestion central.

L'application Web doit être sécurisée au moyen d'un certificat SSL RSA 2048 bits.

Le centre de données à partir duquel s'exécute l'application Web doit être certifié selon une norme ISO 9001 : 2008, OHSAS 18001 : 2007, ISO / IEC 27001 : 2005, ISO 50001 : 2011, ISO 14001, PCI-DSS et FACT.

La disponibilité du centre de données doit être au moins de niveau 3.

Le système de gestion central doit prendre en charge plusieurs niveaux de connexion pour différents utilisateurs.

Le système de gestion central doit prendre en charge l'authentification multifactorielle.

Un certificat d'authentification Open SSL 2048 bits doit être utilisé pour garantir une communication HTTPS fiable avec les systèmes tiers.

Des sauvegardes et des mécanismes de sauvegarde variés doivent être mis en œuvre. Une sauvegarde complète de chaque serveur de base de données doit être effectuée toutes les 24 heures. Ces sauvegardes doivent être disponibles dans le centre de données et doivent être dupliquées sur un stockage externe au siège social du fournisseur du système de gestion central.

# Création et gestion de groupes et de la capacité de stationnement

Un utilisateur doit être en mesure de créer un ou plusieurs groupes de stationnement dans le système de gestion central pour chaque zone de stationnement à destination des différents groupes d'utilisateurs de la zone de stationnement partagée.

Pour chaque groupe de stationnement, il doit être possible de définir une capacité journalière (nombre de places de parking allouées).

Il doit pouvoir être possible de définir un groupe de stationnement comme groupe excédentaire.

Les utilisateurs disposant des droits d'accès appropriés devraient être en mesure de créer des sous-divisions pour un groupe de stationnement afin de subdiviser davantage la capacité du groupe de stationnement.

# Vue d’ensemble et commande à distance

Le système de gestion central doit posséder une page contenant une vue d'ensemble qui montre une représentation graphique de la configuration effective de chaque système d'accès et des groupes de stationnement existants.

La représentation graphique de chaque système d'accès doit montrer la position actuelle effective du système d'accès et l'ajuster en temps réel quand elle évolue.

La vue d'ensemble des systèmes d'accès et leur état de position en cours doit être enrichie d'images d'une ou de plusieurs caméras couvrant une vue d'ensemble, et installées sur les systèmes d'accès.

La vue d’ensemble doit indiquer quelle portion de la capacité désignée a été utilisée et donc combien de places de stationnement sont encore disponibles pour chaque groupe de stationnement.

La vue d’ensemble doit montrer les 5 activités d'accès les plus récentes pour chaque groupe de stationnement.

La vue d'ensemble doit être équipée de commandes pour chaque groupe de stationnement qui peuvent être utilisés pour fournir un accès à distance en ouvrant la barrière et en actionnant les feux de signalisation à bon escient.

La vue d’ensemble doit automatiquement mettre à jour le nombre de places de stationnement occupées et disponibles pour un groupe de stationnement dès qu'un véhicule de ce groupe de stationnement a obtenu un accès automatique ou manuel.

La vue d'ensemble doit avoir une commande d'urgence pour chaque système d'accès qui remplace la politique d'accès standard du système d'accès en question aussi longtemps qu'elle est activée.

En fonction du rôle de l'utilisateur, il doit être possible de limiter la vue d'ensemble avec les systèmes d'accès et les commandes manuelles de ces installations à un sous-ensemble des groupes de stationnement affichés.

La vue d'ensemble doit indiquer qu'il n'y a pas de connexion entre le système de gestion central et l'un des systèmes d'accès au moyen d'un code couleur et d'un texte.

La vue d'ensemble doit indiquer en temps réel qu'un véhicule passe l'un des systèmes d'accès et dans quelle direction.

# Journal de bord des évènements

Les changements d'état de tout le matériel connecté doivent être enregistrés avec une grande précision dans un journal de bord et dans le bon ordre au moyen d'un horodatage, de sorte qu'une image précise du fonctionnement de l'ensemble du système soit par la suite obtenue.

Les utilisateurs doivent pouvoir effectuer une recherche en filtrant des accès, des identifiants, des événements spécifiques et des messages sur l'état du statut d'un matériel spécifique sur une certaine période de temps.

Les informations doivent être stockées localement sur le contrôleur ainsi que dans le système de gestion central et doivent être synchronisées en continu.

Les autorisations pour consulter le journal de bord doivent être définies pour chaque utilisateur dans le système de gestion des utilisateurs du système de gestion central.

Les résultats d'une recherche dans le journal doivent être exportés par l'utilisateur sous forme de fichier CSV avec une commande spécifique.

# Gestion des droits d’accès

Les droits d'accès doivent pouvoir être créés, modifiés et supprimés dans le système de gestion central.

Afin de simplifier la gestion des droits d'accès, l'utilisateur doit être en mesure de mettre en place des modèles qui autorisent tout type de droit d'accès lié à ce modèle à accéder aux mêmes emplacements et aux mêmes heures.

Les droits à visualiser ou à modifier les droits d'accès doivent pouvoir être définis pour chaque utilisateur dans le système d'administration des utilisateurs du système de gestion central.

En fonction du rôle de l'utilisateur, il doit être possible de filtrer les modèles que cet utilisateur peut visualiser et sélectionner lors de la création ou de la modification d'un droit d'accès.

Le système doit prendre en charge plusieurs identifiants pour chaque droit d'accès.

Pour chaque droit d'accès, l'utilisateur doit pouvoir établir une date de début et une date de fin qui détermine la validité dudit droit d'accès.

Pour chaque droit d'accès, l'utilisateur doit sélectionner un groupe de stationnement qui est préconfiguré.

Les droits d'accès qui ont expiré devraient automatiquement être supprimés sous une période de temps configurable, à l'issue de la date de fin de validité.

Les droits d'accès doivent être enrichis par l'utilisateur avec les informations additionnelles souhaitées grâce à l'utilisation de champs libres.

Les utilisateurs devraient pouvoir effectuer des recherches dans la liste des droits d'accès.

La liste des droits d'accès devrait être exportée par les utilisateurs avec une commande spécifique sous la forme d'un fichier CSV.

Le système de gestion central doit fournir à l'utilisateur un aperçu des droits d'accès qui ont été (automatiquement) importés depuis une autre source au moyen de l'API REST.

# Evènements et fenêtres de temps

Les utilisateurs devraient être en mesure de définir des fenêtres de temps standards et récurrentes pendant lesquelles les installations d'accès devraient permettre un libre passage dans le système de gestion central.

Les utilisateurs doivent pouvoir pré-enregistrer les événements qui nécessitent une exception à la politique d'accès standard à un passage dans le système de gestion central afin que les systèmes d'accès sélectionnés fournissent un accès libre aux jours et aux périodes définis.

# Accessibilité des services d’urgence et d’assistance

Le système doit être équipé d'un lecteur capable de lire et d'identifier des transpondeurs spécialement préprogrammés pour les véhicules d'urgence et d'assistance à une distance de 10 mètres, afin que la ou les barrières puissent être ouvertes à temps et que ces véhicules ne soient pas bloqués inutilement.

Les véhicules équipés d'un transpondeur avec ce code spécial doivent à tout moment avoir accès, sans qu'il faille créer un droit d'accès dans le système de gestion central.

Le système de gestion central doit avoir un bouton d'urgence qui permet à un utilisateur de l'application logicielle d'abaisser à distance tous les poteaux rétractables dans l'éventualité d'une urgence jusqu'à ce que ce mode d'urgence soit désactivé.

Le système de gestion central doit indiquer de manière visible dans l'application logicielle si des systèmes d'accès sont en mode d'urgence et quels sont ces systèmes.

# Avertissement

# Ces informations sont fournies à titre indicatif et sans garantie quant à leur exactitude ou leur exhaustivité ; la publication n'accorde pas de licence en vertu d'un brevet ou d'une autre loi, et l'éditeur n'assume aucune responsabilité pour les conséquences de son utilisation ; les précisions et la disponibilité des produits qui y sont énumérés sont susceptibles d'être modifiées sans préavis ; le présent document ne peut être reproduit d'aucune manière, que ce soit tout ou en partie, sans le consentement écrit de son éditeur.

# Document revisies

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Responsable** | **Commentaire** |
| 1.0 | 23-03-2021 | DN | Version initiale |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |