Tender specifications

MOOV Leisure

2021-03-21 | versie 1.0

vehicle acces control

This document is intended to assist professionals in preparing project specifications, requests for information ('RFI') or a proposal ('RFP'), and submissions for tenders for access control systems to regulate vehicle access to recreational parks and sites.

The specifications are classified by subject.

Nedap reserves the right to change this document without prior written notice. The supplier of the specified products can be reached at:

Nedap Identification Systems
P: +31 544 471 111
E: info@nedapidentification.com
http://www.nedapidentification.com

Table of contents

1 Funcional description

The system should be used for selective access of vehicles to a recreation park or a recreational area.

The access of vehicles for this application must be regulated by means of access systems, consisting of one or more barriers that can be operated automatically or manually, and remotely from any location. The access systems must be able to provide automatic access to vehicles with valid access rights, by opening the barrier (s) automatically after identification and verification of means of access.

The system shall support all common means of access, such as license plate recognition, pass cards, transponders, QR codes, Bluetooth and NFC.

In addition to local control, all access systems within the project must be controlled within one central management system for determining and implementing the desired access policy by setting time window, recording authorized means of access and being able to manually operate the barriers remotely.

The central management system must be offered as a Software-as-a-Service (SaaS) solution so that users can access the control panel and access rights management anytime and anywhere via the Internet.

The authorized access means and time window must be continuously synchronized by the central management system with a local storage at the relevant access systems, so that the access control remains operational when an Internet connection is temporarily not possible.

For this purpose, the access systems must be equipped with controllers specifically designed for vehicle access, so-called "vehicle management controllers".

2 Controllers

The type of vehicle management controller must have the following functionalities and properties:

- Local storage of data - including valid means of access, time window, event logging - and automatic synchronization of these with the central management system;
- Connecting and controlling at least two barriers;
- Connecting at least 4 identification readers based on multiple types of identification (i.e., badges, tags, license plate recognition, biometrics, cell phones);
- Connecting license plate cameras via IP;
- Connecting LED traffic lights up to 24V 2x2 (red / green);
- Monitoring correct movement speed and direction of the barrier;
- Proven functioning at an operating temperature of -30 ° C to +60 ° C;
- Protection class IP22 or higher.

3 Central management system

All information regarding access activity at the access systems must be collected and logged on a central Cloud-hosted server.

The supplier must be able to provide both the event log for each access, as well as the manual control of the access systems and the entry and management of access rights, in a single web application.

The central management system should be accessible with any modern web browser that supports Java.

The central management system must use Industry Standard Protocols (such as REST or REST Hooks) to enable integration with third-party booking or reservation systems.

Documentation describing the available REST Hooks must be available and accessible from the central management system.

The web application must be secured by means of an RSA 2048 bits SSL certificate.

The data center where the web application runs must be certified according to ISO 9001: 2008, OHSAS 18001: 2007, ISO / IEC 27001: 2005, ISO 50001: 2011, ISO 14001, PCI-DSS and FACT.

The availability of the data center must be at least Tier 3.

The central management system must support multiple login levels for different users.

The central management system must support two-factor authentication.

An Open SSL 2048-bit trusted certificate should be used to ensure reliable HTTPS communication with third-party systems.

Various backups and backup mechanisms must be implemented. A full backup of each database server should be made every 24 hours. These backups must be available in the data center and must be mirrored to an external storage at the head office of the supplier of the central management system.

4 Creating and managing parking groups and capacity

The central management system must have an overview page that shows a graphical representation of the actual setup of each access system.

The graphical representation of each access system must show the actual current position of the access system and adjust it in real-time when it changes.

The overview of access systems and their current position status should be enriched with images from one or more overview cameras installed at the access systems.

The overview must show the 5 most recent access activities per access system.

The overview must be equipped with buttons for each access system that can be used to provide remote access by opening the barrier and operating the traffic lights in a correct manner.

The overview must have an emergency button for each access system that overrides the standard access policy of the access system in question as long as it is activated.

The overview must indicate by means of color coding and text when there is no connection between the central management system and one of the access systems.

The overview must indicate in real time when a vehicle passes one of the access systems and in which direction.

5 Logging of events

Status changes of all connected hardware must be recorded in a logbook with high accuracy and in the correct order by means of a timestamp, so that an accurate picture of the operation of the system as a whole can be obtained afterwards.
Users must be able to search by means of filters for accesses, identifiers, specific events and status messages of specific hardware within a certain time period.

The information must be stored locally on the controller as well as within the central management system and must be continuously synchronized.

Permissions to view the log must be defined per user in the user management of the central management system.
The results of a search in the logbook should be exported by the user as a .CSV file with one button.

6 Access rights management

Access rights must be able to be created, edited and deleted in the central management system.

In order to simplify the management of access rights, the user should be able to set up templates that allow any access right to which this template is attached to have access at the same locations and at same times.

Rights to view or edit access rights should be able to be determined per user in the user administration of the central management system.

Depending on the role of the user, it must be possible to filter the templates that this user can view and select when creating or editing an access right.

The system must support multiple identifiers per access right.

For each access right, the user must be able to set a start and end date that determines the validity of the respective access right.

Access rights that have expired should be automatically cleared within an configurable period after the end date.

Access rights must be enriched by the user with additional desired information through the use of free fields.

Users should be able to search the list of access rights.

The list of access rights should be exported by users with one button as .CSV file.

The central management system must provide the user with insight into the access rights that have been (automatically) imported from another source by means of the REST API.

7 Events and time windows

Users should be able to set up standard recurring time periods during which access installations should provide free passage in the central management system.

Users must be able to pre-register events that require an exception to the standard access policy at a passage in the central management system so that the selected access systems provide free access within the specified days and time period.

8 Accessibility of emergency and assistance services

The system must be equipped with a reader that can read and identify specially pre-programmed transponders for emergency and assistance vehicles at a distance of 10 meters, so that the barrier (s) can be opened in time and these vehicles are not unnecessarily held up.

Vehicles equipped with a transponder with this special code must be given access at all times, without having to create an access right in the central management system.

The central management system must have an emergency button that allows a user in the software application to remotely lower all retractable posts in the event of an emergency until this emergency mode is canceled.
The central management system must visually indicate in the software application whether and which access systems are in emergency mode.

Disclaimer

Document revisions

Version	Date	Responsible	Comment
1.0	21-03-2021	DN	Initial version