nedap

Ausschreibungs-Unterlagen

MOOV Multi-Tenant

2021-03-29 | version 1.0

vehicle acces control

Dieses Dokument soll Fachleuten bei der Erstellung von Projektspezifikationen, bei Anfragen um Informationen oder Vorschläge sowie bei der Einreichung von Ausschreibungen für Parkverwaltungssysteme für gemeinsam genutzte Parkgelegenheiten behilflich sein.

Die Spezifikationen sind nach Themen geordnet.

Nedap behält das Recht vor, dieses Dokument ohne vorherige schriftliche Ankündigung zu ändern. Der Anbieter der angegebenen Produkte ist erreichbar unter:

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

Inhaltsverzeichnis

1 Funktionsbeschreibung

Das System soll für den selektiven Zugang von Fahrzeugen zu einer gemeinsam genutzten Parkfläche basierend auf einer festgelegten Kapazität pro Benutzergruppe eingesetzt werden.

Der Zugang von Fahrzeugen muss für diese Anwendung mittels Zugangssystemen geregelt werden, welche aus einer oder mehreren Schranken bestehen, die sowohl manuell als auch automatisch und von jedem Ort aus fernbedient werden können. Die Zugangssysteme müssen in der Lage sein, Fahrzeugen mit gültigen Zugangsrechten automatischen Zugang zu gewähren, indem sie die Schranke(n) nach der Identifikation und Verifizierung der Zugangsmittlel automatisch öffnen.

Bevor es Zugang gewährt, sollte das System prüfen, zu welcher Parkgruppe das Fahrzeug gehört und welche Kapazität für diese Parkgruppe verfügbar ist.

Falls sich herausstellt, dass das überprüfte Fahrzeug zu einer Parkgruppe gehört, für die die festgelegte Kapazität bereits erreicht wurde, sollte diesem Fahrzeug kein automatischer Zugang gewährt werden.

Das System muss alle gängigen Zugangsmöglichkeiten unterstützen, wie z.B. Nummernschilderkennung, Passkarten, Transponder, QR-Codes, Bluetooth und NFC.

Zusätzlich zur örtlichen Kontrolle müssen alle Zugangssysteme innerhalb des Projekts von einem zentralen Managementsystem gesteuert werden, um die gewünschten Zugangsrichtlinien durch die Festlegung von Zeitrahmen, die Aufzeichnung von autorisierten Zugangsmittlel und die Möglichkeit, die Schranken manuell aus der Ferne zu bedienen, festzulegen und umzusetzen.

Das zentrale Managementsystem muss als Software-as-a-Service (SaaS) angeboten werden, sodaß die Benutzer zu jeder Zeit und von überall aus durch das Internet Zugriff auf das Control Panel und die Verwaltung der Zugangsrechte haben.

Die Mittel zum autorisierten Zugang und die Zeitrahmen müssen vom zentralen Managementsystem ständig mit einem lokalen Speicher in den entsprechenden Zugangssystemen synchronisiert werden, sodaß die Zugangskontrolle aufrecht erhalten bleibt, wenn eine Internetverbindung vorübergehend nicht möglich ist.

Zu diesem Zweck müssen Zugangssysteme mit so genannten „Fahrzeugmanagement-Controllern“ ausgestattet sein, welche den Zugang von Fahrzeugen steuern.

2 Controllers

Der Fahrzeugmanagement-Controller muss die folgenden Funktionen und Eigenschaften besitzen:

- Lokale Speicherung von Daten – einschließlich gültiger Zugangsmittel, Zeitrahmen, Ereignissprotokollierung und automatischer Synchronisierung dieser Daten mit dem zentralen Managementsystem;
- Verbinden und Steuern von mindestens zwei Schranken;
- Verbinden von mindestens 4 Identifikationslesern basierend auf verschiedenen Arten der Indentifikation (z.B. Dienstmarken, Tags, Nummernschilderkennung, Biometrik, Mobiltelefone);
- Anschließen von Nummernschildkameras über IP;
- Anschließen von LED-Ampeln bis 24V 2x2 (rot- grün);
- Überwachung der korrekten Bewegungsgeschwindigkeit und -Richtung der Schranken;
- Nachgewiesene Funktion bei einer Betriebstemperatur von -30 ° C to +60 ° C ;
- Schutzklasse IP22 or höher.
- Die Möglichkeit, ein Alenco-Schild anzuschließen.

3 Zentrales Managementsystem

Alle Informationen zur Zugangsaktivität auf den Zugangssystemen müssen auf einem zentralen, in der Cloud gehosteten Server gesammelt und protokolliert werden.

Der Anbieter muss in der Lage sein, sowohl das Ereignisprotokoll für jeden Zugang als auch die manuelle Steuerung der Zugangssysteme und die Eingabe und Verwaltung von Zugangssrechten in einer einzigen Webanwendung bereitzustellen.

Auf das zentrale Managementsystem sollte mit jedem modernen Webbrowser zugegriffen werden können, der Java unterstützt.

Das zentrale Mangementsystem muss Industriestandardprotokolle (wie z.B. REST oder REST Hooks) einsetzen, um die Integration in Systeme von Drittanbietern zu ermöglichen.

Dokumentationen, die die verfügbaren REST-Hooks beschreiben, müssen über das zentrale Managementsystem verfügbar und zugänglich sein.

Die Webanwendung muss mit einem RSA 2048-Bit-SSL-Zertifikat gesichert werden.

Das Datenzentrum, in dem die Webanwendung ausgeführt wird, muss gemäß ISO 9001: 2008, OHSAS 18001: 2007, ISO / IEC 27001: 2005, ISO 50001: 2011, ISO 14001, PCI-DSS und FACT zertifiziert sein.

Die Verfügbarkeit des Datenzentrums muss mindestens Tier 3 betragen.

Das zentrale Managementsystem muss mehrere Anmeldeebenen für verschiedene Benutzer unterstützen.

Das zentrale Managementsystem muss die Zwei-Faktor-Authentifizierung unterstützen.

Ein Open SSL 2048-Bit-vertrauenswürdiges Zertifikat sollte verwendet werden, um eine zuverlässige HTTPS-Kommunikation mit Systemen von Drittanbietern sicherzustellen.

Es müssen verschiedene Sicherungskopien und Datensicherungsmechanismen implementiert werden. Eine vollständige Sicherung jedes Datenbankservers sollte alle 24 Stunden durchgeführt werden. Diese Sicherungen müssen im Datenzentrum verfügbar sein und in einen externen Speicher in der Zentrale des Anbieters des zentralen Managementsystems gespiegelt werden.

4 Erstellen und Verwalten von Parkgruppen und -Kapazitäten

Ein Benutzer soll in der Lage sein, eine oder mehrere Parkgruppen pro Parkzone im zentralen Managementsystem für die verschiedenen Benutzergruppen der gemeinsam genutzten Parkfläche zu erstellen.

Es soll möglich sein, für jede Parkgruppe eine tägliche Kapazität (die Anzahl von zugewiesenen Parkplätzen) festzusetzen.

Es soll möglich sein, eine Parkgruppe als eine Überlaufgruppe zu kennzeichnen.

Benutzer mit den entsprechenden Zugangsrechten sollen in der Lage sein, Untergruppen in einer Parkgruppe zu erstellen, um die Kapazität der Parkgruppe weiter aufzuteilen.

5 Ubersicht und Fernbedienung

Das zentrale Managementsystem muss über eine Übersichtsseite verfügen, die eine grafische Darstellung des tatsächlichen Aufbaus eines jeden Zugangssystems und der vorhandenen Parkgruppen enthält.

Die grafische Darstellung jedes Zugangssystems muss die aktuelle Position des Zugangssystems anzeigen und sie bei Änderungen in Echtzeit anpassen.

Die Übersicht über Zugangssysteme und ihren aktuellen Positionsstatus sollte mit Bildern von einer oder mehreren Übersichtskameras angereichert werden, die an den Zugangssystemen installiert sind.

Die Übersicht soll anzeigen, wie viel der festgelegten Kapazität für jede Parkgruppe genutzt wurde, und wieviele freie Parkplätze daher noch verfügbar sind.

In der Übersicht müssen die 5 neuesten Zugangsaktivitäten pro Parkgruppe angezeigt werden.

Die Übersicht muss mit Schalftflächen für jede Parkgruppe ausgestattet sein, mit denen der Fernzugang durch Öffnen der Schranken und die ordnungsgemäße Bedienung der Ampeln ermöglicht werden kann.

Die Übersicht soll automatisch die Anzahl der benutzten und verfügbaren Parkplätze einer Parkgruppe aktualisieren, wenn einem der Fahrzeuge dieser Parkgruppe automatischen oder manuellen Zugang gewährt wurde.

Die Übersicht muss für jedes Zugangssystem eine Notruftaste enthalten, die die Standardzugangssrichtlinien des betreffenden Zugangsssystems überschreibt, solange es aktiviert ist.

In der Übersicht muss mittels Farbcodierung und Text angegeben werden, wenn keine Verbindung zwischen dem zentralen Managementsystem und einem der Zugangssysteme besteht.

Abhängig von der Rolle des Benutzers soll es möglich sein, die Übersicht mit den Zugangssystemen und den Schaltflächen zur manuelle Steuerung dieser Anlagen auf eine Teilmenge der angezeigten Parkgruppen einzuschränken.

Die Übersicht muss in Echtzeit anzeigen, wann und in welche Richtung ein Fahrzeug eines der Zugangssysteme passiert.

6 Protokollierung von Ereignissen

Statusänderungen aller angeschlossenen Hardware müssen mit hoher Genauigkeit und in der richtigen Reihenfolge mittels eines Zeitstempels in einem Logbuch festgehalten werden, damit anschließend ein genaues Bild des Betriebs des gesamten Systems erhalten werden kann.

Benutzer müssen in der Lage sein, innerhalb eines bestimmten Zeitraums mithilfe von Filtern nach Zugriffen, Kennzeichen, bestimmten Ereignissen und Statusmeldungen bestimmter Hardware zu suchen.

Die Informationen müssen lokal auf der Steuerung sowie im zentralen Managementsystem gespeichert und kontinuierlich synchronisiert werden.

Die Berechtigungen zum Anzeigen des Protokolls müssen für jeden Benutzer in der Benutzerverwaltung des zentralen Managementsystems definiert werden.

Die Ergebnisse einer Suche im Logbuch sollten vom Benutzer als CSV-Datei mit einer Schaltfläche exportiert werden.

7 Verwaltung von Zugangssrechten

Zugangsrechte müssen im zentralen Managementsystem erstellt, bearbeitet und gelöscht werden können.

Um die Verwaltung der Zugangsrechte zu vereinfachen, sollte der Benutzer in der Lage sein, Vorlagen einzurichten, die es jedem Zugangsrecht, an das diese Vorlage angehängt ist, ermöglicht, an denselben Orten und zu denselben Zeiten Zugang zu gewähren.

Die Rechte zum Anzeigen oder Bearbeiten von Zugangsrechten sollten für jeden Benutzer in der Benutzerverwaltung des zentralen Managementsystems festgelegt werden können.

Abhängig von der Rolle des Benutzers muss es möglich sein, die Vorlagen zu filtern, die dieser Benutzer beim Erstellen oder Bearbeiten eines Zugangsrechts anzeigen und auswählen kann.

Das System muss mehrere Kennungen pro Zugangssrecht unterstützen.

Für jedes Zugangsrecht muss der Benutzer ein Start- und Enddatum festlegen können, das die Gültigkeit des jeweiligen Zugangsrechts bestimmt.

Der Benutzer muss für jedes Zugangssrecht eine vorkonfigurierte Parkgruppe auswählen.

Abgelaufene Zugangsrechte sollten innerhalb eines konfigurierbaren Zeitraums nach dem Enddatum automatisch gelöscht werden.

Die Zugangsrechte müssen vom Benutzer durch die Verwendung freier Felder mit zusätzlichen gewünschten Informationen erweitert werden.

Benutzer sollten in der Lage sein, die Liste der Zugangsrechte zu durchsuchen.

Die Liste der Zugangsrechte sollte von Benutzern mit einer Schaltfläche als CSV-Datei exportiert werden.

Das zentrale Managementsystem muss dem Benutzer Einblick in die Zugangsrechte geben, die (automatisch) über die REST-API aus einer anderen Quelle importiert wurden.

8 Ereignisse und Zeitrahmen

Benutzer sollten in der Lage sein, wiederkehrende Standardzeiträume einzurichten, in denen Zugangsinstallationen freien Durchgang im zentralen Verwaltungssystem ermöglichen sollen.

Benutzer müssen in der Lage sein, Ereignisse, die eine Ausnahme von den Standardzugangsrichtlinien erfordern, an einer Stelle im zentralen Verwaltungssystem vorab zu registrieren, damit die ausgewählten Zugangssysteme innerhalb der angegebenen Tage und des angegebenen Zeitraums freien Zugang bieten.

9 Zugang von Notfall- und Hilfsdiensten

Das System muss mit einem Lesegerät ausgestattet sein, das speziell vorprogrammierte Transponder für Notfall- und Hilfsfahrzeuge aus einer Entfernung von 10 Metern lesen und identifizieren kann, damit die Schranke(n) rechtzeitig geöffnet werden können und diese Fahrzeuge nicht unnötig aufgehalten werden.

Fahrzeuge, die mit einem Transponder mit diesem speziellen Code ausgestattet sind, müssen jederzeit Zugang haben, ohne dass ein Zugangsrecht im zentralen Managementsystem erstellt werden muss.

Das zentrale Managementsystem muss über eine Notfalltaste verfügen, mit der ein Benutzer in der Softwareanwendung im Notfall alle einziehbaren Pfosten aus der Ferne absenken kann, bis dieser Notfallmodus aufgehoben wird.

Das zentrale Managementsystem muss in der Softwareanwendung visuell anzeigen, ob und welche Zugangssysteme sich im Notfallmodus befinden.

Haftungsklausel

Dokumentenrevision

Version	Datum	Verantwortlicher	Kommentar
1.0	23-03-2021	DN	Initial version