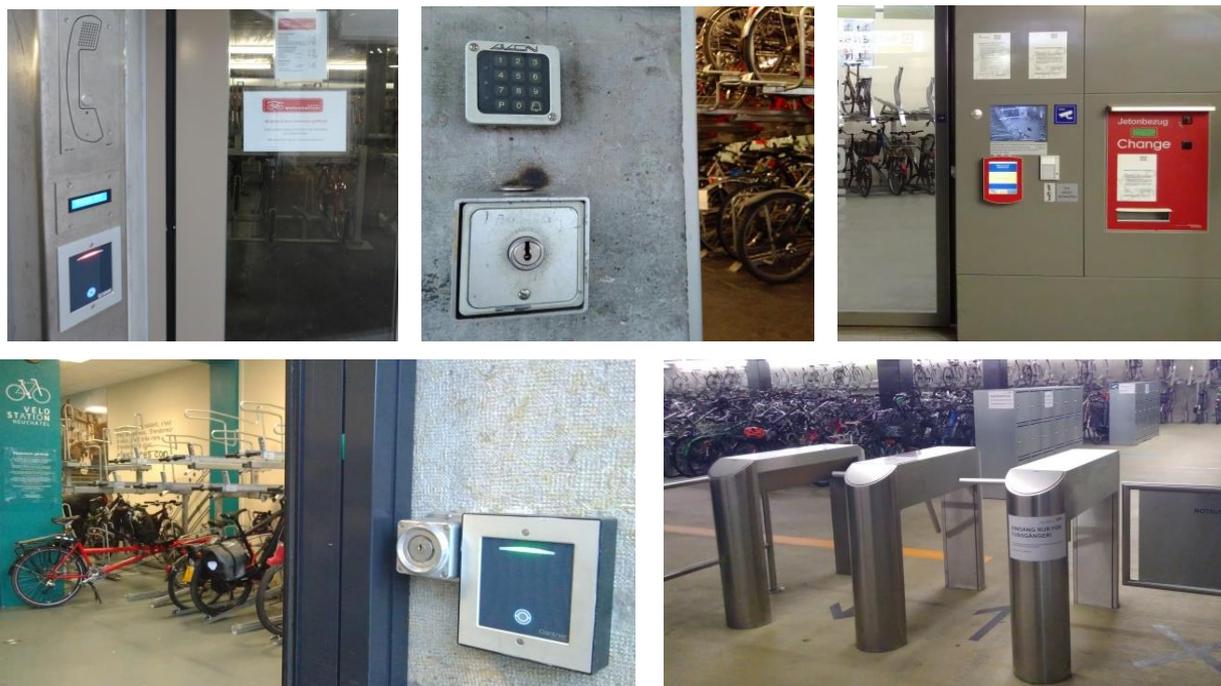


Projet harmonisation de la gestion des accès vélostations

Cahier des charges du système uniformisé

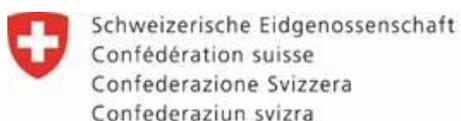
Partie gestion des accès



Nils Rinaldi, Valérie Sauter, Martin Wälti, Anita Wenger

Berne, le 31 mai 2018

Avec le soutien de :



Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC



Table des matières

1. Introduction	3
2. Fonctionnement de la vélostation « minimale »	6
3. Options supplémentaires pour vélostation avec plus de service	7
3.1 Vélos avec tag UHF pour ouverture longue distance	7
3.2 Gestion des casiers	7
3.3 Porte d'entrée équipée de sas	7
4. Architecture du système de gestion des accès	8
5. Besoins logiciels	10
5.1 Application du contrôle des accès avec monitoring des événements	10
5.2 Interface avec le système de gestion des utilisateurs	10
6. Besoins matériels	12
6.1 Contrôle d'accès	12
6.2 Lecteur longue distance pour les vélos (optionnel)	14
6.3 Puces RFID pour les vélos (optionnel)	14
6.4 Casiers (optionnel)	14
7. Maintenance et service après-vente	15
8. Garantie	16
9. Indicateur de prix	17
10. Glossaire	19
Impressum	20

1. Introduction

PRO VELO Suisse a initié le projet « Vélostations: optimisation des systèmes d'accès et compatibilité au niveau national ». Ce projet a pour but de contribuer à l'optimisation des systèmes d'accès des vélostations et d'initier une harmonisation de la gestion des accès aux vélostations en Suisse. Ceci notamment afin d'en simplifier l'exploitation et d'en rendre la gestion moins coûteuse. Un catalogue des besoins, ainsi que deux cahiers des charges ont été rédigés dans le cadre de ce projet et permettront aux fournisseurs de mieux cerner les besoins des vélostations et de proposer des produits adaptés. Ces documents simplifieront également le processus d'implémentation de systèmes d'accès pour les communes. Une première évaluation des systèmes d'accès et de gestion des utilisateurs sur le marché a été faite via une demande d'informations menée auprès de différents fournisseurs. Le processus de mise en œuvre d'un système central de gestion des accès, non compris dans ce projet, pourra être défini sur la base des résultats obtenus.

Ce projet est coordonné par le Forum vélostations Suisse. Il est soutenu par l'Office fédéral des transports dans le cadre des projets retenus par le Bureau de coordination pour la mobilité durable COMO. Il reçoit également le soutien de l'Union des transports publics UTP, des CFF, de Caritas Lucerne, du Conseil régional du district de Nyon, du canton de Bâle-Ville, ainsi que des villes de Berne, Berthoud, St-Gall, Thun et Zurich.

La première phase du projet a consisté à réunir les besoins en fonctionnalités pour un tel système uniformisé. Cette phase a débouché sur un document appelé « définition des besoins et fonctionnalités », disponible sur le site www.velostation.ch/fr/documents.

Dans ce document des besoins est présentée une architecture générique souhaitée du système uniformisé, avec un **système de gestion des utilisateurs central unique**, et un **système de gestion des accès par vélostation**. Le point commun entre ces systèmes de gestion des accès est qu'ils acceptent les **mêmes média d'identification**, à savoir la carte **SwissPass** et le **smartphone**.

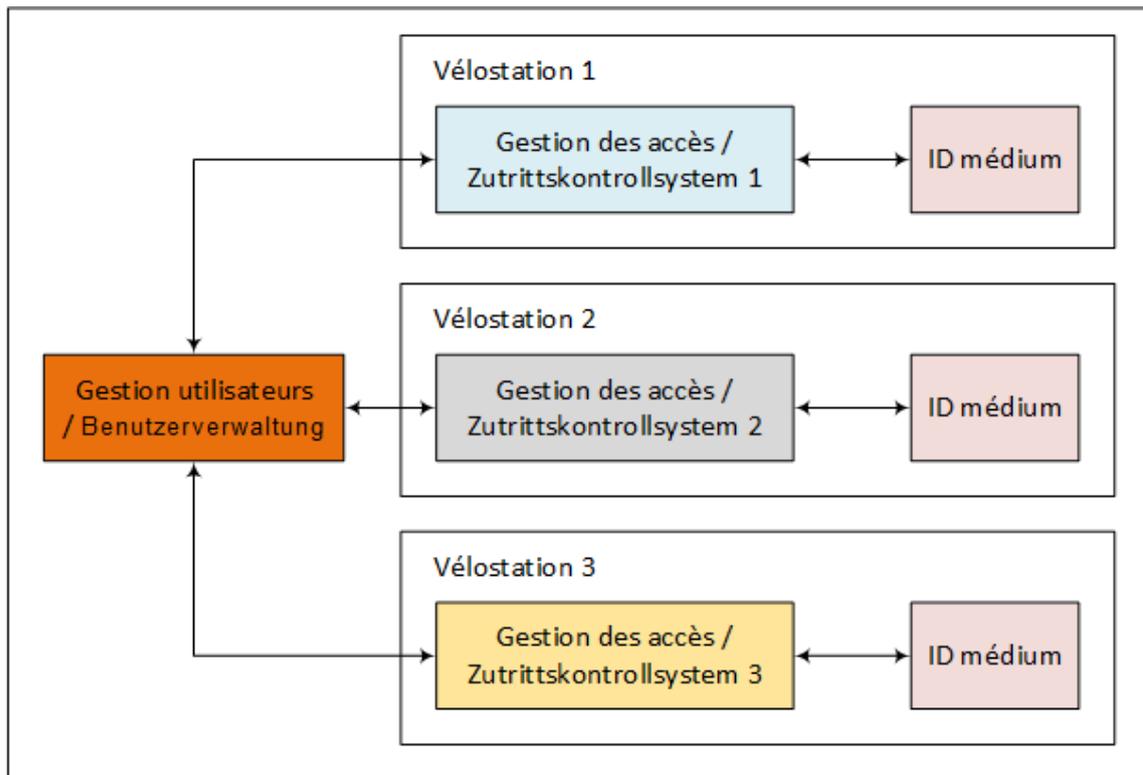


Figure 1: Gestion des utilisateurs centralisée et plusieurs systèmes de gestion des accès

Le présent document **définit le cahier des charges de la partie « gestion des accès » uniquement**. Il est destiné aux vélostations qui souhaitent effectuer un appel d'offre auprès de fournisseurs susceptibles de pouvoir offrir une telle solution respectant ce cahier des charges. La partie « gestion des utilisateurs » fait l'objet d'un document séparé, également disponible sur www.velostation.ch/fr/documents.

La figure suivante décrit plus en détails l'architecture globale du système. Elle définit en bleu le périmètre du présent document, à savoir la partie de gestion des accès.

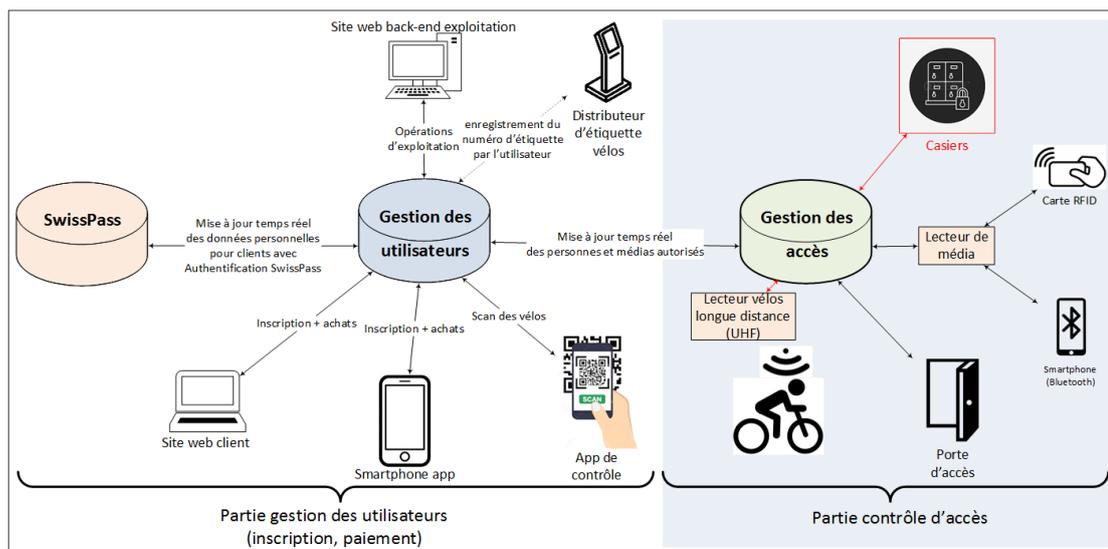


Figure 2: Cahier des charges du système "gestion des accès": périmètre

L'hypothèse de départ est la volonté de déterminer les conditions nécessaires à la mise en place d'un **système qui puisse servir une vélostation « minimale »**, c'est-à-

dire sans exploitation humanisée quotidienne, et offrant uniquement les services obligatoires tels que définis dans le document de définition des besoins. Ce système sera considéré comme la colonne vertébrale minimale. Le fonctionnement de base de cette vélostation est décrit au chapitre 2.

Autour de cette colonne vertébrale minimaliste pourront **se greffer des services complémentaires** tels qu'équipement des vélos de tags UHF (longue distance) pour ouvrir la porte en pédalant, casiers pour casques, etc. Ces services sont décrits au chapitre 3.

Le chapitre 4 décrit la vue d'ensemble (**architecture**) des deux types de vélostations (« minimale » ou avec guichet). Le chapitre 5 définit les **besoins logiciels**, alors que le chapitre 6 définit les **besoins matériels**. Le chapitre 7 décrit les **besoins de service après-vente**.

2. Fonctionnement de la vélostation « minimale »

L'hypothèse de départ est que la vélostation n'est pas exploitée humainement, elle est de type **autonome**.

Il y a un **contrôle d'accès physique « classique »** à l'entrée de la vélostation, avec un lecteur sachant lire **une carte SwissPass ou un smartphone**. Ce système de contrôle d'accès gère **la porte d'entrée principale** à travers laquelle l'utilisateur et le vélo entreront. Il n'y a donc pas de porte dédiée pour l'utilisateur, et de porte dédiée pour le vélo.

La porte n'est a priori pas équipée de « sas » à l'entrée, ce qui ne garantit pas que la personne qui y rentre, soit seule. Ceci implique que des personnes mal intentionnées puissent se glisser à l'intérieur de la vélostation. Il est donc recommandé de coupler le système de contrôle d'accès à un **système de vidéosurveillance** (qui ne fait pas partie de ce cahier des charges).

L'utilisateur gère son compte Vélostation à l'aide d'une **application smartphone dédiée**, ou à l'aide d'une **page web semblable**. Lors de la création de son compte, il **y associe** soit sa carte SwissPass, soit son smartphone (ou même les deux).

L'utilisateur déjà inscrit, et qui se présente (le matin avant le travail typiquement) à la vélostation, s'authentifie à la porte d'entrée en présentant sa carte SwissPass ou son smartphone. La porte s'ouvre, et il rentre ensuite avec son vélo dans la vélostation, et la porte se referme derrière lui. Ensuite, **lorsqu'il quitte la vélostation, il presse sur un bouton de sortie** (pas besoin d'authentification à la sortie) pour ouvrir la porte et quitter le bâtiment.

L'utilisateur qui revient récupérer son vélo (le soir typiquement après sa journée de travail) s'authentifie à la porte d'entrée en présentant sa carte SwissPass ou son smartphone. Il rentre dans la vélostation, récupère son vélo, ressort en pressant le bouton de sortie.

D'autres moyens d'accès que le SwissPass ou le smartphone peuvent être utilisés en parallèle par les vélostations (tickets, clés, jetons,...), mais ceux-ci ne sont pas gérés par le système central de gestion des utilisateurs et n'auront pas de fonction en dehors de la vélostation qui les utilise.

L'exploitant de la vélostation dispose d'**outils de reporting online**, lui permettant de contrôler le bon fonctionnement de sa vélostation, et son taux d'utilisation.

Le système de **vidéosurveillance** (ne faisant pas partie de ce cahier des charges) permet également à l'exploitant de gérer les cas de vols éventuels.

3. Options supplémentaires pour vélostation avec plus de service

3.1 Vélos avec tag UHF pour ouverture longue distance

Le système de contrôle d'accès dans ce cas est équipé d'un second lecteur RFID (en plus du lecteur RFID traditionnel), de type UHF (Ultra High Frequency), permettant une lecture d'un tag UHF attaché au vélo, à une distance de 5-10 mètres. Ceci permettrait à l'utilisateur d'entrer dans la vélostation en pédalant, sans devoir descendre du vélo, ni sortir son SwissPass ou son smartphone.

3.2 Gestion des casiers

Un service de casiers peut être mis à disposition des utilisateurs. Il doit être compatible avec le système de contrôle d'accès de la porte de la vélostation, c'est-à-dire que l'utilisateur doit pouvoir utiliser la même carte SwissPass ou smartphone qu'il a utilisé pour entrer dans la vélostation, pour s'attribuer un casier, ou ouvrir un casier déjà attribué.

3.3 Porte d'entrée équipée de sas

Idéalement, la porte d'entrée ne devrait laisser passer qu'une seule personne à la fois, ceci pour garantir la sécurité des vélos à l'intérieur de la vélostation, et pour prévenir la fraude. Ceci n'est possible que par l'installation d'un système de sas à double porte, forçant le passage d'une personne à la fois. C'est une mesure mécanique (et non technologique) à mettre en œuvre.

4. Architecture du système de gestion des accès

Le système de gestion des accès est composé, au minimum, des éléments suivants :

- **Logiciel de gestion des accès**, qui permettra à l'exploitant de la vélostation de gérer ses utilisateurs, et monitorer l'utilisation de sa vélostation. Il est composé d'une base de données, ainsi que d'une application offrant une interface utilisateur permettant d'interagir avec le système ;
- **Interfaces** avec les systèmes externes :
 - o Avec le système de gestion des utilisateurs, au travers de web services exposés par le système de gestion des accès, et appelés par le système de gestion des utilisateurs ;
 - o Avec le matériel électronique qui gère physiquement les accès des portes.
- **Matériel** : contrôleur, lecteur de carte RFID et de smartphone, gâche d'ouverture de porte, et en option senseur de porte, radar de détection de présence

Un **système de vidéosurveillance**, complètement découplé des éléments listés ci-dessus, et ne faisant pas partie du présent cahier des charges, complète le système informatique d'exploitation de la vélostation.

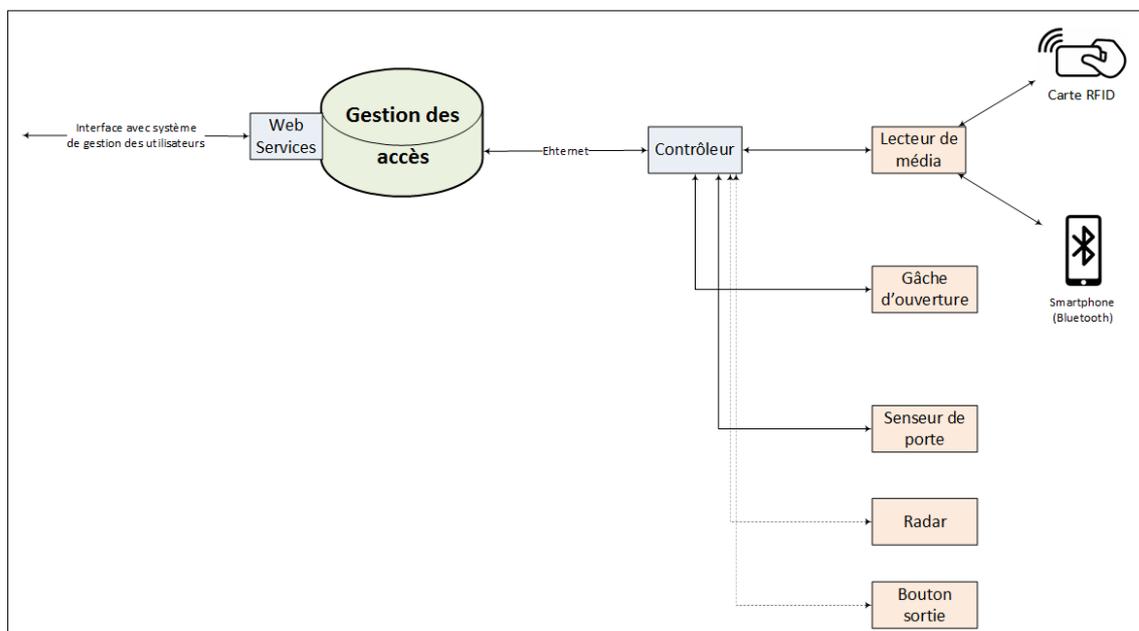


Figure 3: Architecture du système de gestion des accès

Le système doit être **évolutif**, c'est-à-dire qu'il doit pouvoir supporter :

- un grand nombre d'utilisateurs (> 50'000),
- permettre l'association de plusieurs médias d'identification par utilisateur,
- un grand nombre de portes (> 2'000).

Le système doit intégrer un **système de monitoring** des événements (accès ok/nok, porte forcée, porte ouverte trop longtemps, batterie faible, etc.), avec possibilité de classement des niveaux d'alerte (3 niveaux suffisants). Il doit permettre l'envoi de SMS / e-mails pour les alertes les plus prioritaires.



Le système doit suivre les standards de **sécurité informatique** en vigueur. Le transfert de données entre les différents composants du système doit impérativement être crypté de bout en bout avec un algorithme reconnu.

Le système doit être **auditable**, c'est-à-dire qu'il sache **loguer toute opération** effectuée dans le système, que ce soit par un utilisateur, par un administrateur ou par un autre système (via interface). Ces logs doivent être exploitables par du reporting dédié à cet effet (afin de les rendre lisible).

5. Besoins logiciels

5.1 Application du contrôle des accès avec monitoring des événements

5.1.1 Introduction

Cet outil est en principe fourni conjointement avec le hardware de contrôle des accès. Il est en général composé d'une base de données, et d'un élément de traitement des données (intelligence).

Il doit présenter des web services permettant à l'outil de gestion des utilisateurs de communiquer avec, notamment pour rajouter des utilisateurs dans le système de contrôle d'accès, de modifier des utilisateurs existants, de rajouter ou modifier des droits d'accès à un utilisateur associé à une carte SwissPass ou un smartphone.

5.1.2 Données stockées

Le système de gestion des accès stocke en général les **données suivantes** :

- Liste des **portes** en accès contrôlé, avec notamment les attributs suivants :
 - o ID de la porte
 - o Description de la porte
 - o Calendrier d'accès libre

- Liste des **utilisateurs**, avec notamment les attributs suivants :
 - o ID utilisateur
 - o Nom, prénom
 - o Média ID 1 (SwissPass)
 - o Média ID 2 (smartphone)
 - o Média ID 3 (UHF tag sur vélo)
 - o Liste des autorisations d'accès

- Liste des **événements**, avec notamment les attributs suivants :
 - o Date de l'événement
 - o Type d'événement (entrée acceptée, sortie acceptée, entrée refusée, sortie refusée, etc.)
 - o ID de la porte sur laquelle a eu lieu l'événement

5.1.3 Contraintes légales

En plus de respecter la loi cantonale de protection des données concernée, le logiciel de gestion des accès devra être conforme à la loi fédérale sur la protection des données (LPD - <https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html>), ainsi que la nouvelle loi européenne General Data Protection Regulation (GDPR - - <https://www.eugdpr.org/>). Il s'agira notamment de bien archiver et anonymiser les données transactionnelles.

5.2 Interface avec le système de gestion des utilisateurs

Le système de contrôle d'accès doit exposer des web services que le système de gestion des utilisateurs doit pouvoir exploiter, afin de pousser des données vers le système de gestion des accès. Sans entrer dans des détails techniques, les web services suivants doivent être fournis :



- **Authenticate** -> pour l'authentification du système de gestion des utilisateurs, la première fois qu'il se connecte aux web services du système de contrôle d'accès ;
- **Add_User** -> permet de rajouter un nouvel utilisateur dans le système de contrôle d'accès, en fournissant les paramètres suivants : ID utilisateur, nom, prénom, et les média IDs nécessaires ;
- **Modify_User** -> permet de modifier les données d'un utilisateur existant déjà dans le système de contrôle d'accès ;
- **Deactivate_User** -> permet de désactiver un utilisateur déjà existant ; ce dernier ne pourra plus accéder à la vélostation ;
- **Reactivate_User** -> permet de réactiver un utilisateur qui avait été auparavant désactivé ;
- **Add_Rights** -> permet de rajouter des droits d'accès à un utilisateur existant ;
- **Modify_Rights** -> permet de modifier des droits d'accès existants à un utilisateur existant.

6. Besoins matériels

6.1 Contrôle d'accès

Une porte de contrôle d'accès online se compose en général d'un contrôleur (relié à la base de données par connexion ethernet RJ45), d'un lecteur, d'un système de verrouillage de porte (gâche électrique, ventouse magnétique, etc.), et d'un capteur de porte ouverte (magnétique, mécanique, etc.). Dans le cas d'une porte automatique (ouverte par moteur), un radar de détection de mouvement est également connecté au contrôleur. Un second radar peut aussi être nécessaire pour la sortie. Il est aussi possible qu'il faille installer un bouton de sortie, dans le cas où la porte n'est pas équipée de radar de sortie, ni de poignée mécanique de sortie.

Le transfert des données entre lecteur, contrôleur et base de données, doit être **crypté** à l'aide d'un algorithme reconnu et réputé indéchiffrable.

Le système de contrôle d'accès proposé pour une porte online doit pouvoir gérer les **configurations** suivantes :

- Gestion d'une porte entrée simple (un lecteur, un système de verrouillage, et un capteur de porte),
- Gestion d'une porte entrée-sortie (deux lecteurs de part et d'autre de la porte, mais un seul système de verrouillage et un seul capteur de porte),
- Gestion d'un buzzer pour alarme porte ouverte trop longtemps,
- Gestion d'une porte automatique avec radar de détection de mouvement.

Le système de contrôle d'accès doit pouvoir gérer plusieurs portes sur un même site (possibilité d'avoir plusieurs portes en accès contrôlé dans une même vélostation). Le système doit permettre d'octroyer à un utilisateur des droits d'accès à plusieurs portes.

Le système de contrôle d'accès doit pouvoir résister à une coupure de courant (utilisation de batteries), ainsi qu'à une coupure de réseau (données d'accès stockées en local dans le contrôleur).

6.1.1 Lecteur de média

L'utilisateur qui souhaite entrer dans la vélostation doit pouvoir s'identifier soit avec sa carte SwissPass, soit avec son smartphone (via connexion Bluetooth).

La carte SwissPass comporte deux puces RFID : une de type Mifare Classic, et une de type SkiData.

Le lecteur de contrôle d'accès doit dès lors supporter les standards suivants :

- Mifare Classic (respecte le standard ISO 14443A partiellement seulement)
- Mifare DESFire - dans un souci d'évolutivité, ce standard étant la génération plus avancée du Classic (conforme en intégralité au standard ISO 14443A)
- SkiData (conforme en intégralité au standard ISO 15693)
- Smartphone (par connexion Bluetooth)

Le lecteur proposé doit pouvoir indiquer l'état de la porte comme par exemple avec deux leds (une verte et une rouge), fonctionnant de la manière suivante :

- accès libre = led verte continue,
- accès contrôlé = aucune led allumée,

- entrée acceptée = led verte pendant quelques secondes,
- entrée refusée = led rouge pendant quelques secondes.

Le lecteur doit être programmable pour qu'il n'accepte que les cartes RFID de type ISO 15693 (même s'il sait aussi lire les cartes de type ISO 14443). En effet, il s'avère que la lecture de la carte SwissPass (qui comporte deux puces RFID différentes) peut présenter des performances moyennes, à cause de l'interférence entre les deux puces. Si le lecteur est paramétré pour ne lire qu'une seule des deux puces, il présentera de meilleures performances.

6.1.2 Gâche d'ouverture

La gâche d'ouverture doit être adaptée à la porte mécanique que présente la vélostation. Elle peut être soit mécanique, soit une ventouse magnétique, soit une simple impulsion vers un moteur de porte automatique.

6.1.3 Senseur de porte

Le senseur de porte doit s'adapter au type de porte que présente la vélostation. Il est en général soit mécanique, soit magnétique.

6.1.4 Radar de détection de mouvement

Le radar de détection de mouvement, qui est pertinent pour une porte automatique motorisée, est en général de type infrarouge. Normalement il y en a un en entrée, et un en sortie.

6.1.5 Bouton de sortie

Dans le cas d'une porte qui n'est pas équipée avec un radar de porte, ni de poignée de sortie, alors il faut y installer un bouton de sortie, afin que l'utilisateur puisse sortir de la vélostation. Le fournisseur du système de contrôle d'accès doit de toute manière s'assurer que les normes de sécurité seront appliquées, afin de garantir que la personne peut sortir de la vélostation (en cas d'incendie par exemple). Ceci peut être fait en installant une barre anti-panique, ou un bouton « verre à briser ».

6.1.6 Contrôleur

Le **contrôleur** doit présenter les fonctionnalités suivantes :

- Il devra utiliser le protocole TCP/IP pour toutes ses communications. Les fonctionnalités du protocole TCP/IP doivent correspondre aux standards du marché.
- Il doit pouvoir continuer à fonctionner lors d'une panne électrique (mode dégradé), grâce à une alimentation secourue.
- Il doit pouvoir continuer à fonctionner lors d'une panne réseau, grâce à une sauvegarde locale des droits d'accès (la mise à jour de droits ne pouvant évidemment pas être prises en compte pendant la panne réseau).
- Il doit être compatible avec le lecteur décrit précédemment.
- Il doit être compatible avec la gâche d'ouverture de porte décrite précédemment.
- Il doit être compatible avec le senseur de porte décrit précédemment.
- Il doit être compatible avec le radar de détection de mouvement décrit précédemment.
- Il doit être compatible avec le bouton de sortie décrit précédemment.

6.2 Lecteur longue distance pour les vélos (optionnel)

Dans le cas où il est souhaité que l'utilisateur puisse accéder à la vélostation sans descendre de son vélo, il est nécessaire d'installer une antenne RFID longue portée, de type UHF, à l'entrée de la vélostation, ainsi qu'une puce RFID UHF active. Cette combinaison permet une grande distance de lecture, et elle est typiquement utilisée sur les péages d'autoroutes pour les abonnés.

La norme UHF fonctionne dans la gamme de fréquence 865-868 MHz (en Europe). Associée à un tag UHF actif, elle permet une lecture allant jusqu'à 10 mètres.

Le lecteur UHF à installer sur le système de contrôle d'accès ne remplace pas le lecteur décrit au chapitre 6.1.1, car ce dernier reste indispensable lorsque l'utilisateur entre dans la vélostation pour récupérer son vélo.

6.3 Puces RFID pour les vélos (optionnel)

Le lecteur UHF décrit précédemment fonctionne à grande distance avec un tag RFID UHF actif. Ce tag doit naturellement être compatible avec le lecteur RFID UHF proposé.

6.4 Casiers (optionnel)

Le système de casiers est en général composé d'un module de gestion et des casiers eux-mêmes. Ces derniers sont soit équipés de lecteurs RFID individuellement, soit équipés d'un lecteur RFID commun pour un certain nombre de casiers. Le système proposé doit être compatible avec les médias d'identification tels que listés au chapitre 6.1.1.

Une solution de contrôle d'accès de type offline n'est pas possible dans le cas présent, vu que la mémoire de la carte SwissPass n'est pas accessible. Il faut donc privilégier une solution online.

7. Maintenance et service après-vente

Le fournisseur du système de gestion des accès doit pouvoir offrir un service après-vente (SAV) sur le système de contrôle d'accès qu'il propose. Dans le cadre de son service après-vente, le fournisseur doit pouvoir garantir les éléments suivants :

- prise en charge d'un incident dans les 2 heures après notification ;
- résolution du problème dans les 24 heures après notification ;
- intervention 7 jours sur 7 de 8h à 19h
- intervention sur tout le territoire suisse urbanisé, en particulier pour ce qui concerne les parties hardware (partie contrôle d'accès) du système.

Les conditions de SAV doivent figurer dans un contrat de SLA (Service Level Agreement) qui doit être mis en place avec le fournisseur, afin de déterminer les conditions de service après-vente, respectant au minimum les éléments listés ci-dessus.



8. Garantie

Le fournisseur s'engage à fournir un software et un hardware qui est supporté pendant les 10 ans suivant leur mise en place respective.

En particulier, le hardware doit être compatible avec le software dans les 10 ans après installation (i.e. le fournisseur ne peut pas forcer le client à changer de matériel pour des raisons de compatibilité avec le software, sauf si ce changement est offert par le fournisseur).

9. Indicateur de prix

Ce paragraphe a pour but de lister les différents éléments qui entrent dans le calcul du budget de l'installation d'un système de contrôle d'accès. Il est utile pour un exploitant de vélostation qui souhaite établir un appel d'offre auprès de fournisseurs potentiels, afin d'avoir des points de comparaison objectifs entre les solutions proposées par les fournisseurs.

Objet	Précisions	Prix unitaire CHF HT
Licence du logiciel de contrôle d'accès	On premise ou Software as a Service (SaaS) ? Coût de licence «one-shot», ou leasing annuel?	
Licence par utilisateur back-office	Inclus dans la licence initiale ou non?	
Licence par utilisateur dans le système de la vélostation	Inclus dans la licence initiale ou non?	
Licence de l'interface web services pour connexion au système de gestion des utilisateurs	Inclus dans la licence initiale ou non?	
Coûts de maintenance annuelle du logiciel	Applicable si licence logicielle «one-shot»	
Licence pour une porte en accès contrôlé	Prix unique, ou dépend des options de la porte?	
Licence du logiciel de vidéosurveillance		
Contrôleur	Combien de portes peut-il gérer?	
Lecteur de média (RFID + Bluetooth)		
Gâche mécanique d'ouverture de porte		
Ventouse magnétique d'ouverture de porte		
Senseur de porte magnétique		
Détecteur de mouvement (radar)		
Bouton de sortie		
Lecteur RFID UHF	Si prix disponible	
Tag RFID UHF	Si prix disponible	
Licence du logiciel de gestion		



des casiers		
Module de gestion des casiers	Si nécessaire dans la solution proposée	
Lecteur RFID pour casier		
Caméra IP		
Coût d'installation d'une porte	Estimation pour une porte simple	
Coût du contrat de maintenance logiciel	Préciser sa couverture	
Coût du contrat de maintenance matériel	Préciser sa couverture	
Coût de gestion de projet en plus-value	Tarif horaire	
Coût d'intervention d'un technicien en plus-value	Tarif horaire	
Coût de formation sur le système	Tarif horaire	

10. Glossaire

Abréviation	Signification
Bluetooth	Standard de communication radio, dans la bande 2.4 GHz, destiné aux connexions courte distance
CSN	Card Serial Number – numéro de carte RFID unique – semblable à UID
CRM	Customer Relationship Management – outil informatique
HF	High Frequency RFID – 13.56 MHz – pour lecture jusqu'à ~30cm
IP	Internet Protocol
ISO 14443A	Standard RFID, dans la gamme de fréquence HF. En général destiné aux personnes.
ISO 15693	Standard RFID, dans la gamme de fréquence HF. En général destiné aux objets.
RFID	Radio Frequency IDentification
SAV	Service Après-Vente
SLA	Service Level Agreement
UHF	Ultra High Frequency RFID – 865-868 MHz– pour lecture à plus longue distance
UID	Unique ID : numéro de carte RFID unique – semblable à CSN

Impressum

Éditeurs

PRO VELO Suisse, 3013 Berne, www.velostation.ch, info@velostation.ch

Avec le soutien de

Office fédéral des transports (OFT)
Chemins de fer fédéraux (CFF)
Union des transports publics (UTP)
Villes de Berne, Berthoud, St-Gall, Thun et Zurich
Canton de Bâle-Ville
Caritas Lucerne
Conseil régional du district de Nyon

Auteurs

Nils Rinaldi (consultant technique)
Valérie Sauter (PRO VELO Suisse)
Martin Wälti (Büro für Mobilität AG)
Anita Wenger (PRO VELO Suisse)

Responsable du projet

Valérie Sauter (PRO VELO Suisse)

Groupe de suivi

Christophe Baumann (Fondation intact); Sven Balsiger (Ville de Thun); Daniel Bartelt (vélostation de St. Gall); Urs Grüter (Caritas Lucerne); Jürg Steiner (vélostation de Berne); Stephanie Stotz (Ville de Berne); Roman Weber (Ville de Zurich)

Téléchargement

www.velostation.ch

Cette publication est aussi disponible en allemand.

Pour des raisons de lisibilité, l'utilisation conséquente des formulations masculines et féminines n'a pas été appliquée.