STid
Electronic Identification

STid Mobile ID®

Bluetooth® Smart

Contrôle d'accès sécurisé et intuitif avec smartphones

Solutions mobiles Bluetooth®

NOTE D'APPLICATION / FAQ

Table des matières

I. Introduction

Ce document décrit l'approche à adopter pour aborder un projet d'identification de personnes à l'aide de la solution d'accès mobile Bluetooth® STid Mobile ID®, afin d'obtenir un résultat optimal en fonction de la configuration et des contraintes de l'installation.

II. Principes généraux de la technologie Bluetooth® Smart

Le Bluetooth® est un standard de communication utilisant des ondes radio sur une bande de fréquence de 2,4 à 2,5 GHz.

La solution STid Mobile ID® utilise cette technologie pour authentifier un utilisateur via une application installée sur son smartphone.

Pour les applications de contrôle d'accès, les distances de lecture sont un facteur primordial. Avec la technologie Bluetooth®, les distances annoncées sont informatives et définissent une zone de détection. Elles dépendent du smartphone et de son positionnement par rapport au lecteur. Par exemple, un téléphone tenu à la main ou dans la poche ne sera pas détecté à la même distance.

III. Questions fréquentes

A. Application STid Mobile ID®

1. Qu'est-ce que l'application STid Mobile ID® ?

L'application STid Mobile ID® est un portefeuille virtuel de badges d'accès. Elle peut recevoir et stocker un nombre illimité de badges. Chaque badge virtuel porte un identifiant sécurisé, programmé par le client/utilisateur ou prédéfini.

2. Avec quelles plateformes mobiles STid Mobile ID® est compatible ?

STid Mobile ID® est téléchargeable sur les plateformes Google Play (Android) et App Store (iOS). 95% des smartphones du marché fonctionnent avec l'un de ces 2 systèmes d'exploitation.

STid Mobile ID® est compatible avec les smartphones Bluetooth® Smart à partir des versions : Android 5.0 et iOS 9.0.

3. Combien coûte l'application STid Mobile ID® ?

L'application STid Mobile ID® est gratuite. Un badge virtuel CSN gratuit - STid Mobile ID® - est directement stocké dans l'application avec un numéro unique attribué à l'installation.

B. Interopérabilité

1. Quels sont les lecteurs compatibles avec STid Mobile ID® ?

Tous les modèles de la gamme Architect® Blue et Architect® One Blue sont compatibles avec l'application STid Mobile ID®.

ARC1S/BT

ARCS-A/BT

ARCS-B/BT

ARCS-C/BT

2. Est-ce que la solution est compatible avec d'autres lecteurs Bluetooth® du marché ?

Afin de garantir les meilleurs niveaux de sécurité et de supporter l'ensemble des fonctionnalités offertes par la solution STid Mobile ID®, seuls les lecteurs de la gamme Architect® Blue et Architect® One Blue sont compatibles avec la solution STid Mobile ID®.

3. Est-ce que la solution est compatible avec les badges d'accès traditionnels ?

Oui, les lecteurs Architect® Blue et Architect® One Blue supportent de nombreuses technologies : Bluetooth® Smart (4.0), NFC (Near Field Communication), toutes les puces 13,56 MHz MIFARE® (Classic, Classic EV1, Ultralight®, Ultralight® C, MIFARE® Plus, MIFARE® Plus EV1, DESFire® EV1 & EV2, DESFire® 256…), les puces iCLASS® / PicoPass® (en CSN uniquement) et les cartes de santé CPS3.

4. Est-ce que la solution d'accès mobile fonctionne avec tous les systèmes de contrôle d'accès ?

Les lecteurs de la gamme Architect® Blue sont identiques aux lecteurs de la gamme Architect® et conservent les mêmes compatibilités systèmes.

Au même titre que toutes les solutions d'accès STid, STid Mobile ID® fonctionne avec tous les systèmes de contrôle d'accès. Les lecteurs sont disponibles en version TTL (Wiegand / Data Clock – ISO2) et en liaison série RS485. L'encodeur dispose d'un câble USB.

C. L'ergonomie

1. Qu'apporte votre solution mobile par rapport à une solution d'accès RFID traditionnelle ?

STid Mobile ID® contribue à l'acceptation de la Politique de Sécurité dans les organisations. Son ergonomie rend l'identification instinctive. STid offre de nombreux modes d'identification qui permettent de vous identifier sans devoir sortir votre téléphone, que celui-ci soit en veille ou en communication.

2. Qu'est-ce que le mode Badge ?

Vous présentez votre smartphone devant le lecteur comme un badge traditionnel RFID.

3. Qu'est-ce que le mode Slide ?

Un simple passage de la main sur le lecteur vous ouvre les portes, en gardant le téléphone dans votre poche ou sac à main. Les technologies capacitives brevetées présentes sur le lecteur permettent de réveiller le lecteur et de démarrer la communication avec le smartphone.

Mode non disponible sur l'ARC1S ni sur l'ARCS clavier en mode Badge ou Touche.

4. Qu'est-ce que le mode Tap Tap ?

Vous tapotez 2 fois le smartphone dans la poche pour une ouverture à proximité ou à distance.

5. Qu'est-ce que le mode Mains-libres ?

Vous passez simplement devant le lecteur, sans aucune action de votre part.

6. Qu'est-ce que le mode Remote ?

Vous utilisez le smartphone comme une télécommande pour contrôler vos points d'accès à distance.

7. Peut-on activer tous les modes d'identification sur un lecteur ?

L'utilisation de plusieurs modes est tout à fait possible pour s'adapter à la politique de sécurité de votre entreprise. A noter toutefois que l'association de certains modes est déconseillée :


+

=

Déconseillé

Le mode mains-libres prend le dessus sur les autres modes puisqu'il ne requiert aucune action pour que l'utilisateur soit authentifié.


+

=

Déconseillé

Obligation de sortir son téléphone pour le déverrouiller.


+

=

Conseillé

Utilisation du mode contact et/ou Slide et/ou TapTap pour le contrôle d'accès bâtiment et du Remote pour l'accès parking.

8. Lorsque le lecteur autorise le mode Slide, est-ce normal que plusieurs téléphones à proximité soient authentifiés ?

Oui, l'utilisateur réveille le lecteur en passant la main. Cette action initialise l'action avec tous les téléphones dans la zone de lecture, ayant l'application active, la fonction Bluetooth® activée et un badge virtuel avec le code site et les clés correspondants à la configuration du lecteur.

9. Que se passe-t-il si le mode Slide et la lecture de badges RFID sont activés sur un même lecteur ?

L'approche du badge RFID vers le lecteur déclenchera la fonction Slide si celle-ci est activée sur le lecteur car ce dernier détectera également la présence de la main. Si l'application mobile est active à proximité du lecteur, le badge RFID sera lu en premier puis l'authentification par le mode Slide prendra effet.

10. Que se passe t'il quand ApplePay est configuré ou le NFC activé sur un téléphone Android ?

Quand l'ApplePay est configuré, votre carte de paiement peut apparaître quand vous présentez le téléphone au lecteur. C'est normal car le lecteur réveille la carte en NFC. Cependant, cela ne génèrera aucune transaction.

Quand le NFC est activé sur un téléphone Android™, et si le lecteur est configuré pour lire également le NFC, vous pourrez avoir des conflits car le lecteur cherchera à lire les deux numéros.

11. Peut-on installer plusieurs lecteurs Architect® Blue & Architect® One Blue dans une même zone ?

Oui, grâce aux technologies exclusives et brevetées STid, vous pouvez discriminer les accès en fonction de leur distance et/ou en changeant le code site.

Selon le mode de lecture choisi, le lecteur ne lira que si on a effectué une action volontaire avec son smartphone et à la distance choisie.

Une distance minimum est à respecter entre deux lecteurs dès lors que l'un des deux est configuré avec un mode « mains-libres ».

12. Peut-on régler les distances de lecture ?

Oui, les distances de lecture vont de 0 à 20 mètre(s) et sont réglables pour chaque mode.

13. Est-ce que la solution fonctionne téléphone en veille ?

Oui, l'ensemble des modes d'identification fonctionne téléphone en veille ou actif, verrouillé ou déverrouillé dans la limite offerte par la version du téléphone et de son OS.

14. Est-ce que l'application mobile consomme beaucoup de batterie ?

La technologie Bluetooth® Smart a pour particularité de ne pas consommer beaucoup. Comme toutes les applications – l'utilisation de la batterie par l'application dépend de la fréquence d'utilisation.

15. Que se passe-t-il si le téléphone n'a plus de batterie ?

Vous ne pouvez pas utiliser votre smartphone pour vous identifier. La technologie Bluetooth® Smart fonctionne uniquement avec le téléphone allumé. Il est conseillé d'utiliser un badge RFID de réserve le cas échéant.

16. Que faire si le téléphone ne s'authentifie plus ?

Il faut tout d'abord :

- Vérifier que les modes « Avion », « Ne pas déranger » ou « Ultra Eco Energie » ne soient pas activés.

- Vérifier que le Bluetooth® soit bien activé.
- Vérifier que l'application mobile soit bien active.

Si le problème perdure après ces étapes de vérification, vous devez redémarrer l'application et/ou réactiver le Bluetooth® et/ou redémarrer le smartphone.

D. La sécurité

1. Comment sont sécurisées les données stockées dans l'application ?

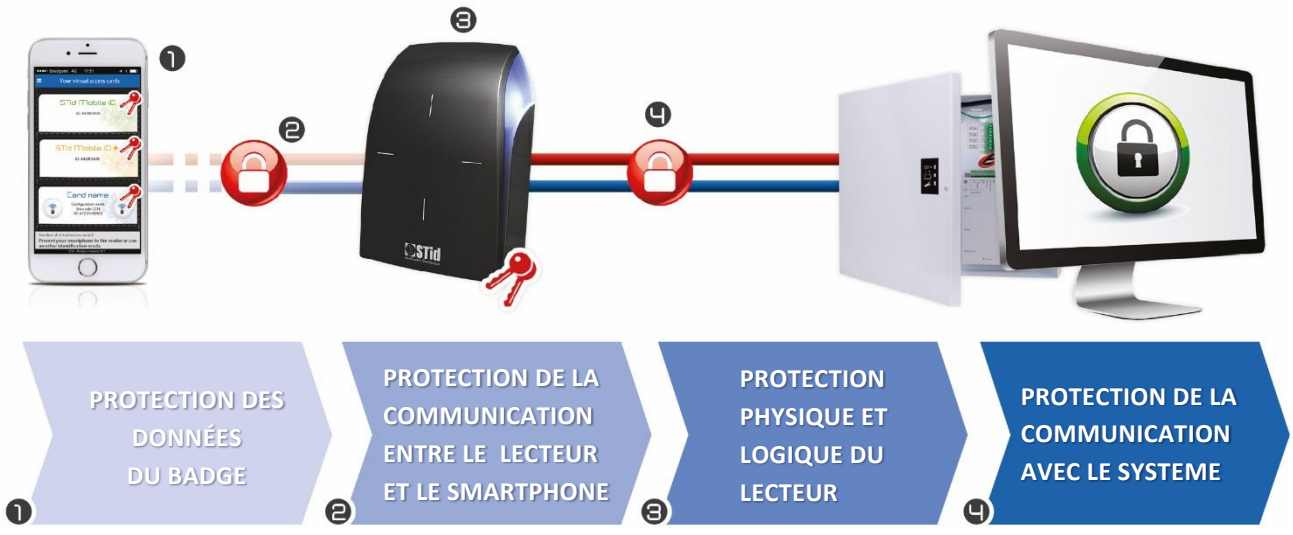
STid assure la protection des données stockées dans l'OS du smartphone par des méthodes de chiffrement (AES 128), d'authentification (SHA-256) et de sécurisation du code. Elles utilisent des algorithmes publics conformes au RGS (Référentiel Général de Sécurité) publié par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour chiffrer et authentifier les données dans l'application à l'aide d'une clé unique à chaque utilisateur.

STid vous offre la possibilité d'ajouter des niveaux de sécurité supplémentaires en imposant le déverrouillage du smartphone (authentification par code PIN, biométrie, reconnaissance vocale…).

2. Comment sont sécurisées les échanges de données ?

Entre le smartphone et le lecteur

STid assure la protection des échanges de données par des méthodes de chiffrement (AES 128), d'authentification (SHA-256) et de sécurisation du code. Elles utilisent des algorithmes publics conformes au RGS (Référentiel Général de Sécurité) publié par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour chiffrer et authentifier les données dans l'application à l'aide d'une clé unique à chaque utilisateur.



3. Comment sont sécurisées les données stockées dans le lecteur ?

Les données sensibles sont stockées dans un composant certifié EAL5+ (même niveau de sécurité que dans le domaine bancaire).

Chaque lecteur Architect® Blue & Architect® One Blue dispose d'un système anti-arrachement innovant par capteur de mouvement. Il protège les données sensibles en permettant d'effacer les clés d'authentification (système breveté). Contrairement aux solutions existantes du marché (interrupteur mécanique, capteur optique, interrupteur à lame souple...), la fiabilité de la technologie par accéléromètre évite tout contournement du système.

Vous pouvez également ajouter des niveaux de sécurité supplémentaires via les modules additionnels des lecteurs : clavier standard ou aléatoire.

4. Comment garantissez-vous la sécurité des données ?

Notre application mobile STid Mobile ID® subit des audits externes réguliers pour garantir un niveau de sécurité constant.

E. Gestion des badges virtuels

1. Qu'est-ce qu'un badge virtuel ?

C'est la dématérialisation de vos badges de contrôle d'accès au sein d'une application mobile. Votre badge virtuel porte un identifiant et se comporte comme un badge RFID.

2. Quels sont les types de badges virtuels disponibles ?

STid vous propose 3 types de badges d'accès adaptés à vos besoins :

Le Badge STid Mobile ID+ est une évolution du badge STid Mobile ID® et donc conserve le même numéro.

3. Quel est l'outil pour gérer les badges virtuels ?

Vous pouvez configurer vos badges virtuels à l'aide de **SECard :**

- Programmation cloisonnée 100% locale
- Maîtrise complète des paramètres de sécurité et de configuration
- Plug & Play sans aucun développement

4. Comment commander les crédits et les charger dans l'encodeur ?

Pour commander des badges virtuels, il est nécessaire d'effectuer une requête de demande de crédits via le Kit de Programmation SECard. Attention, la demande de crédits doit être accompagnée d'une commande à adresser à votre revendeur.

1. • Connexion de l'encodeur au PC
   • Sélection du nombre de crédits dans SECard
   • Génération de la requête
2. Envoi de la commande de crédit avec le fichier « Credit Request » à votre revendeur
3. Réception du code de rechargement de crédit par email
4. Chargement des crédits dans l'encodeur

5. Quelle est la valeur des crédits ?

- 1 "upgrade" STid Mobile ID+ = 1 crédit
- 1 badge Virtual access card = 5 crédits

6. Où sont stockés les crédits ?

En mode Offline, vos crédits sont stockés de manière sécurisée dans le composant crypto processeur EAL5+ de l'encodeur associé à votre Kit de programmation SECard.

7. Comment j'utilise les crédits ?

Lors de l'encodage des badges virtuels avec SECard, les crédits correspondant au type de badge créé sont débités automatiquement de l'encodeur.

8. Que se passe-t-il si l'encodeur tombe en panne ?

Nous avons la possibilité en usine de retrouver le nombre de crédits restant sur un encodeur en panne. En cas de destruction de l'encodeur cela deviendra impossible et le solde de crédits sera perdu.

9. Comment créer, modifier et supprimer les badges virtuels ?

En mode Offline, vous devez utiliser le Kit de programmation SECard Blue pour gérer vos badges virtuels. L'utilisateur a la possibilité de supprimer le badge virtuel stocké dans son smartphone via l'application.

Lors d'une suppression, nous vous conseillons de supprimer l'ID de votre système de contrôle d'accès comme pour un badge de contrôle d'accès classique.

10. Qu'est-ce qu'il se passe si l'application est désinstallée ?

Tous les badges stockés dans l'application seront supprimés et perdus au moment de la désinstallation.

11. Qu'est-ce qu'il se passe si l'on perd le téléphone ?

En mode Offline, vous devez supprimer l'ID du système au même titre que si vous perdiez votre carte RFID. Il faut ensuite créer un nouveau badge virtuel.

12. Comment faire pour migrer des badges RFID MIFARE® DESFire® sur les smartphones ?

Une fonction de SECard vous permet de reprendre les paramètres de vos badges DESFire® dans les smartphones. Votre configuration actuelle DESFire® sera déclinée d'un simple clic et vous pourrez alors programmer des ID Virtuels dans vos smartphones qui seront immédiatement reconnus par vos lecteurs, sans redéfinir de paramétrage spécifique.

F. Configuration des lecteurs d'accès

1. Quels sont les outils qui permettent de configurer les lecteurs ?

Vous configurez vos lecteurs Bluetooth® avec le même outil que pour les autres lecteurs STid 13,56 MHz MIFARE® : le kit de programmation SECard. Il permet de créer les badges maîtres physiques ou virtuels de configuration des lecteurs (incluant paramètres et clés).

Vous configurez vos lecteurs à l'aide d'un badge physique RFID ou virtuel via l'application STid Settings.

2. Qu'est-ce que l'application STid Settings ?

STid Settings est un portefeuille virtuel de badges de configuration permettant de les stocker dans votre smartphone et de paramétrer les lecteurs en toute simplicité.

3. Avec quelles plateformes mobiles STid Settings est compatible ?

STid Settings est téléchargeable sur les plateformes Google Play (Android™) et App Store (iOS). 95% des smartphones du marché fonctionnent avec l'un de ces 2 systèmes d'exploitation.

4. Combien coûte l'application STid Settings ?

L'application STid Settings est gratuite.

5. Est-ce que je consomme des crédits quand je crée des badges virtuels de configuration dans l'application STid Settings ?

Non, la création de badges virtuels de configuration est gratuite. Vous pouvez en créer un nombre illimité.

G. Compatibilités avec les smartphones

Des différences de comportement / performances peuvent apparaître en fonction du modèle et de la version du téléphone et de son système d'exploitation.

Cependant, afin de vous garantir la meilleure expérience d'utilisation, nous réalisons des tests sur un large éventail de téléphones pour appréhender leur comportement. Vous trouverez ci-après les modèles qualifiés par STid.

Nexus	6P	Android 7.0	
	6	Android 7.0	
	6	*Android 5.x*	*Non Fonctionnel*
Huawei	P9	Android 7	Lenteurs constatées
Samsung	S6	Android 6	
	S7	Android 6	
	S7	Android 7	
	S4	Android 5	
	A5	Android 6	Lenteurs constatées

iPhone	5C	iOS 10.2.1	
	5S		
	6		
	6+		
	6S+		
	7		
	7+	iOS 10.3	

Note 1 : Liste évolutive.

Note 2 : Liste non exhaustive : Les applications peuvent fonctionner sur des smartphones non présents dans cette liste.

IV. Approche des projets

Il convient de respecter certaines étapes lorsqu'on souhaite équiper un site, nouveau ou existant, avec une configuration Bluetooth®.

A. Analyse du site

Tous les lecteurs d'un même site ne seront pas obligatoirement configurés avec les mêmes modes et distances d'authentification.

Il est nécessaire de recenser les informations de base nécessaires à la définition de la (des) configuration(s) à retenir :

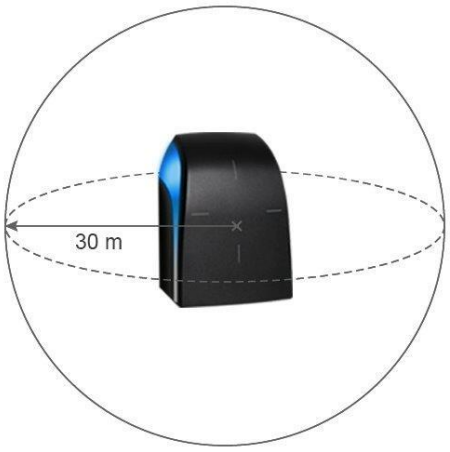
- Plan de site
- Sens de circulation
- Définir pour chaque lecteur le(s) modes et distances d'authentification
- Nombre d'accès à sécuriser
- Nombre de personnes à identifier
- Parc de smartphones

B. Définir les tests

Dès le départ, nous recommandons de définir les tests nécessaires à la validation de la configuration avec le client.

C. Notes importantes

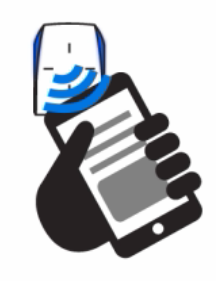
- En fonctionnement, les lecteurs Bluetooth® émettent de façon sphérique autour du lecteur.



- Les distances de détection dépendent du modèle de smartphone et de son positionnement par rapport au lecteur.
- L'identification de personnes est une action volontaire. Elle nécessite l'activation du Bluetooth® et de l'application STid Mobile ID® sur le smartphone.

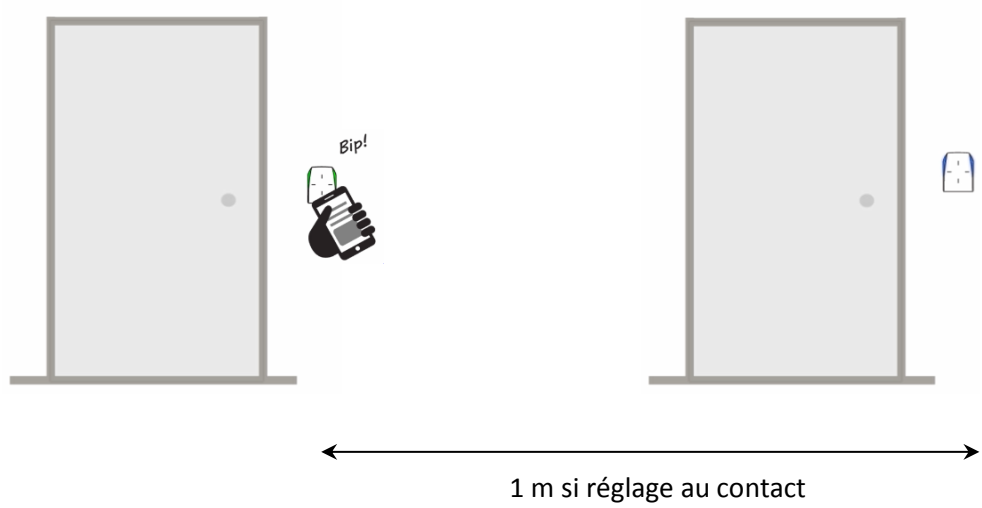
V. Mode Badge

Le smartphone est utilisé comme un badge de contrôle d'accès physique.



Ce mode d'identification pourra être utilisé dans les cas suivants :

A. Installation de plusieurs lecteurs à proximité



L'authentification ne se fait ainsi que sur un lecteur.

B. Installation avec demande d'authentification forte

Dans ce cas, il faut activer l'option imposant le déverrouillage du téléphone pour que le lecteur s'authentifie avec le badge.

Selon les smartphones, le déverrouillage peut se faire par empreinte digitale, par code PIN, par reconnaissance vocale ou par schéma.

Attention : cette fonctionnalité n'est pas utilisée par défaut sur les smartphones, il est donc nécessaire de l'activer.

VI. Exemple sur une installation type

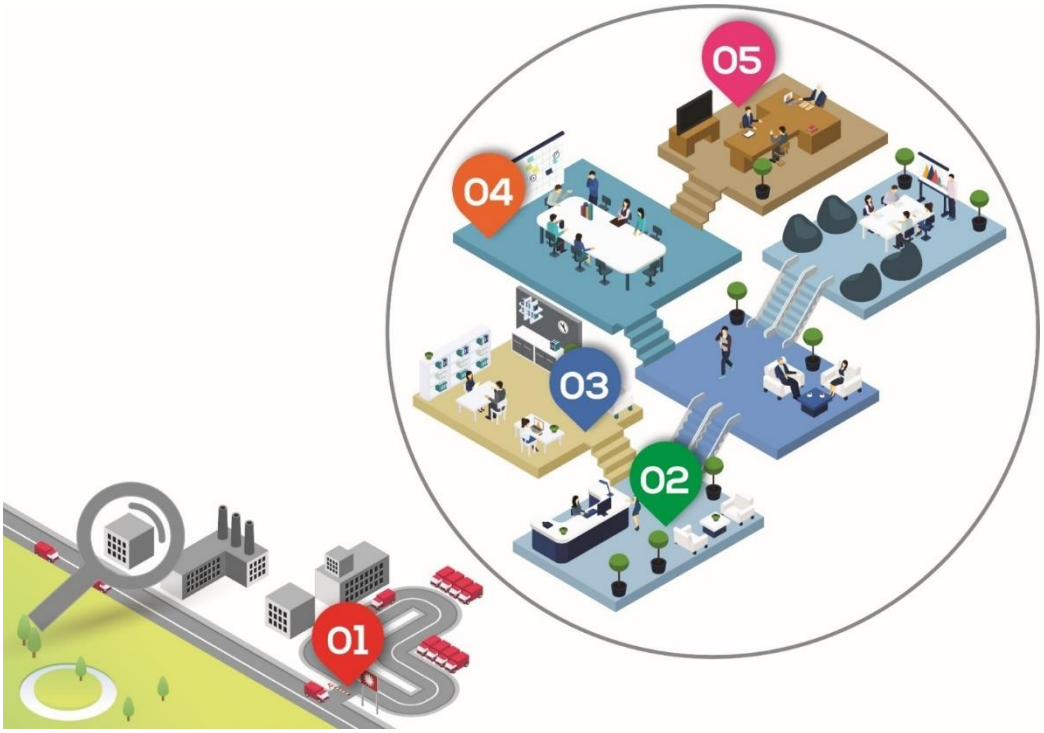
A. Analyse de site

1. Plan de site

- Sens de circulation

Point d'accès		Sens de circulation	Mode d'identification	Nom de la configuration
01	Accès Parking	Entrée et Sortie	Remote Mains-libres	Parking Entrée Parking Sortie
02	Entrée / Accueil	Entrée	Badge Tap Tap	Accueil
03	Salle serveur	Entrée	Badge avec déverrouillage du téléphone	Serveur
04	Salle de réunion	Entrée	Badge Slide	Bureau 1
05	Bureau Direction	Entrée	Badge Slide	Bureau 2

- Définir pour chaque lecteur le(s) mode(s) et distance(s) d'identification



2. Définir les tests

Point d'accès		Contrainte	Distance	Test
	Accès parking	Accès Voiture/Vélo/Moto Entrée et sortie donc 2 configurations	Remote : jusqu'à 20m Mains-Libres : jusqu'à 3m	Vérifier que les distances soient adaptées à votre application. Si trop grandes ou trop courtes ajuster les distances dans la configuration.
	Entrée / Accueil	Aucune / pas de lecteur à moins de 4 mètres	Badge : jusqu'à 0.50m TapTap : jusqu'à 3m	Vérifier que les distances sont correctes, si trop grandes ou trop courtes ajuster les distances dans la configuration.
	Salle serveur	Authentification forte Lecteur 4 à moins de 3 mètres	Badge : contact Nécessite le déverrouillage du téléphone pour lancer l'authentification	
	Salle de réunion	Lecteur 3 à moins de 3 mètres	Badge : contact Slide : très proche	Ajuster la distance du slide pour que le lecteur ne s'authentifie pas avec le téléphone de la personne du bureau voisin.
	Bureau Direction	Aucune / pas de lecteur à moins de 2 mètres	Badge : jusqu'à 0.50m Slide : très proche	

B. Paramètres des badges d'accès virtuels

Il faut :

- Définir le nom du badge virtuel : par exemple « Acces STid ».
- Configurer les paramètres de sécurité du Blue Mobile ID : une clé / deux clés et renseigner la (les) clé(s).
- Faire apparaitre les boutons Remote pour l'accès parking.

C. Configuration des lecteurs avec SECard

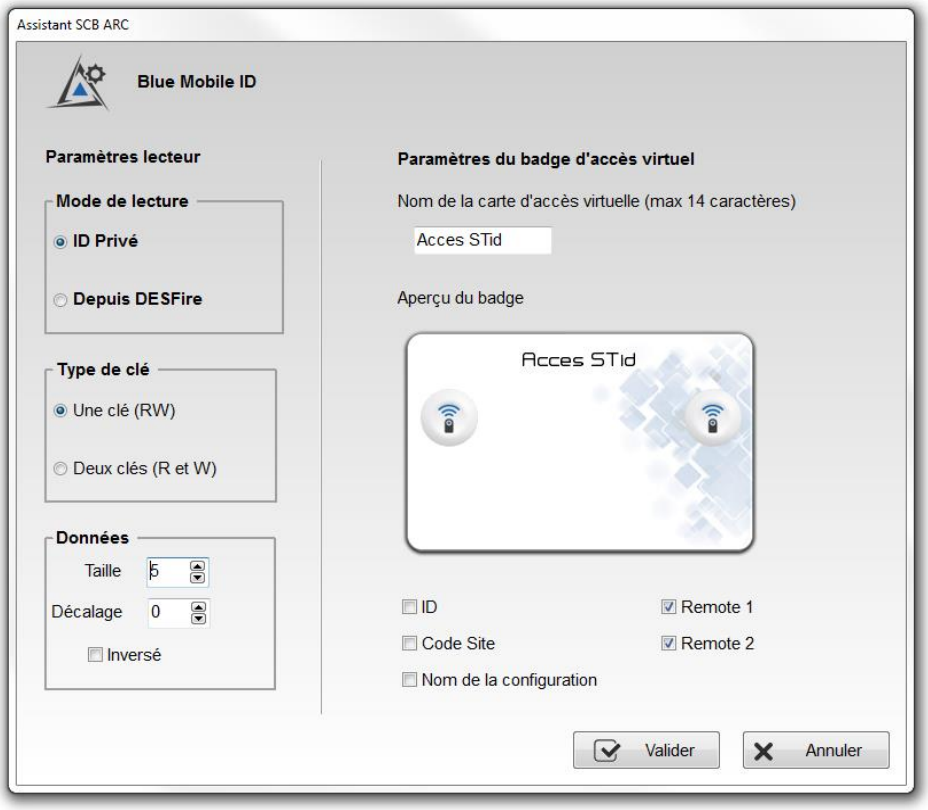
Il faut définir un code site pour l'installation. A titre d'exemple, nous choisirons « 5A5B ».

Nous aurons donc 6 badges de configuration à créer. Pour cela, STid propose 2 supports :

- Badge virtuel avec l'application gratuite STid Settings - les badges SCB virtuels sont gratuits et leur stockage est illimité.
- Badge MIFARE® DESFire® EV1 - prévoir un nombre suffisant de badge DESFire® EV1 4Ko CCTW380.

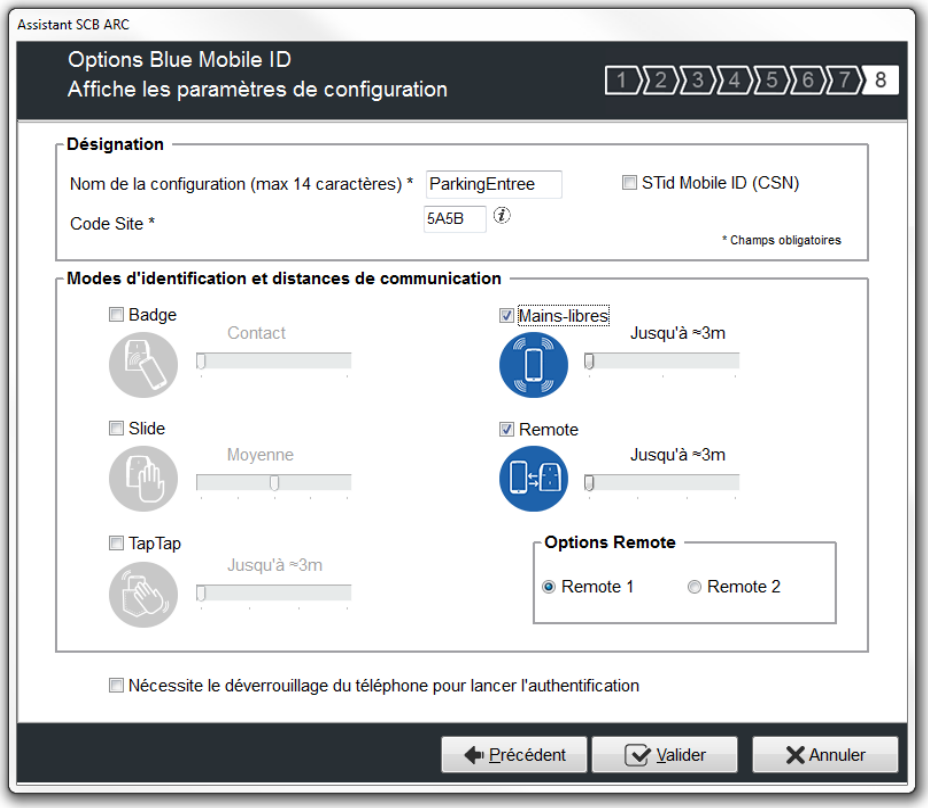
Pour chacune des configurations présentées, il faut créer le badge de configuration correspondant avant de passer à la nouvelle.

1. Paramètres SECard pour la création des badges virtuels utilisateurs



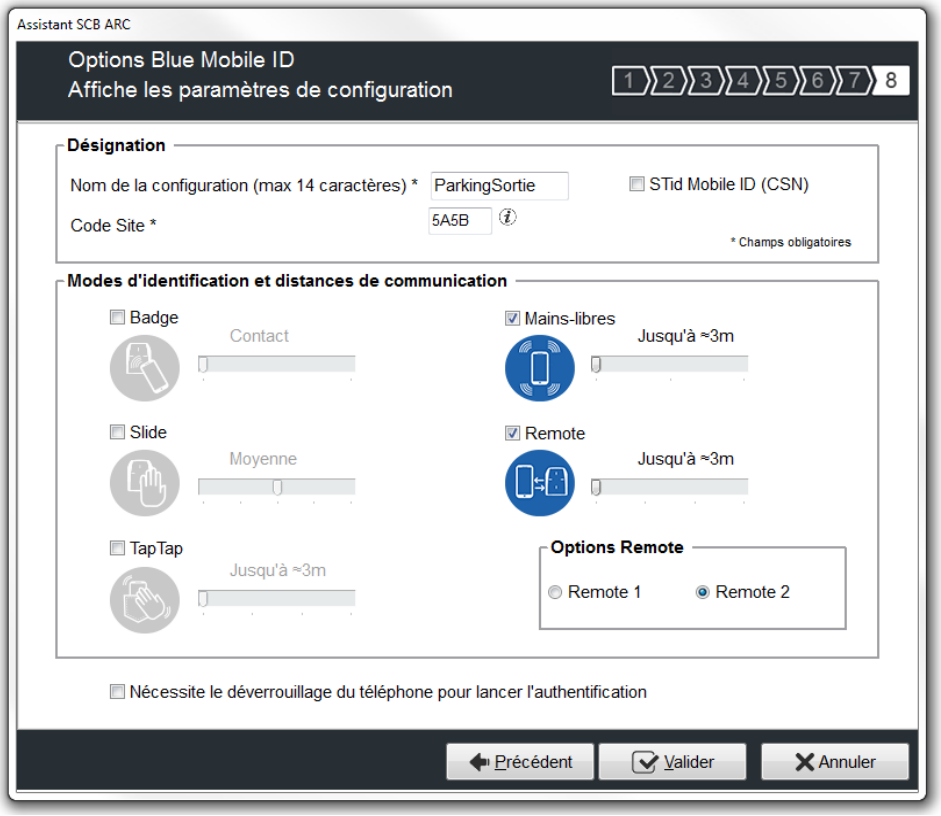
2. Paramètres SECard pour la création du badge de configuration Parking Entrée

Le bouton 1 sera attribué au lecteur d'entrée

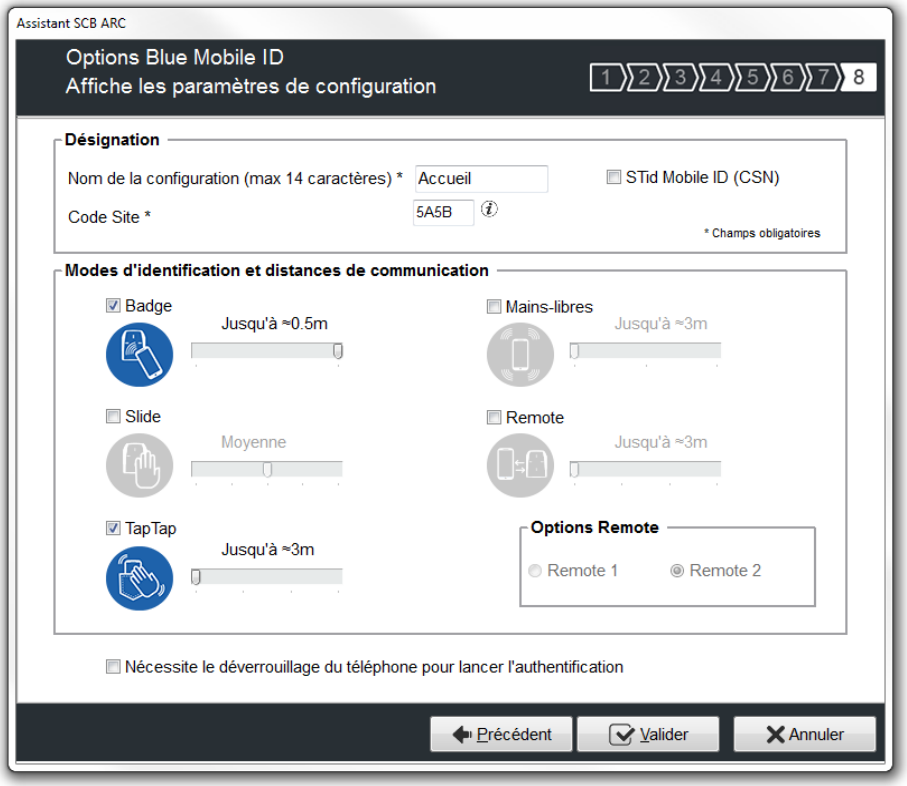


3. Paramètres SECard pour la création du badge de configuration Parking Sortie

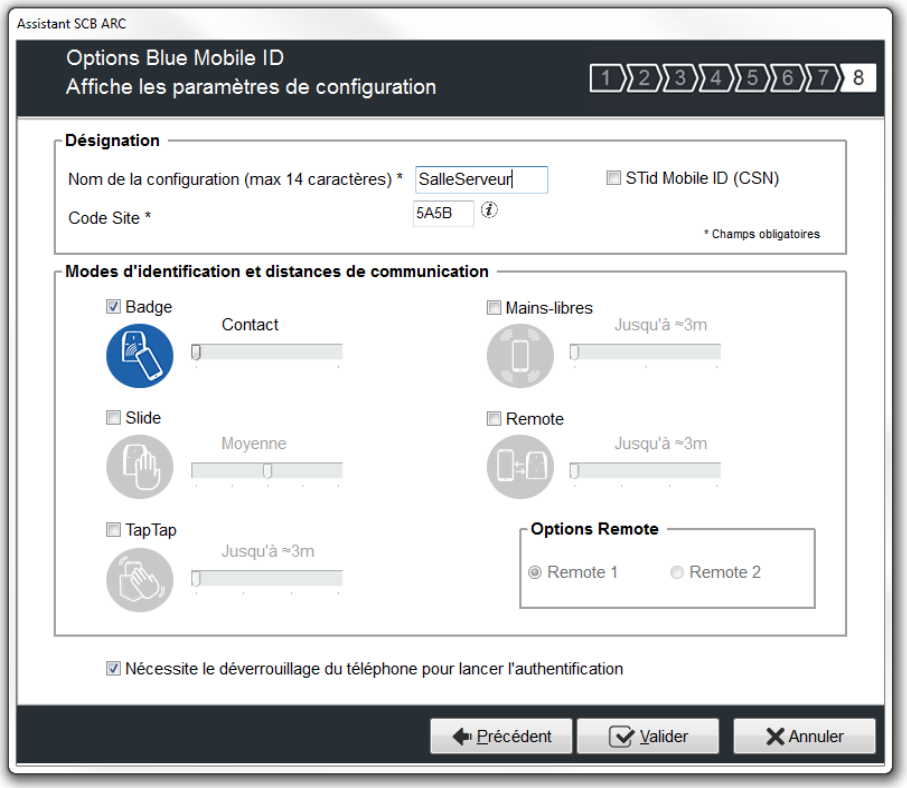
Le bouton 2 sera attribué au lecteur de sortie.



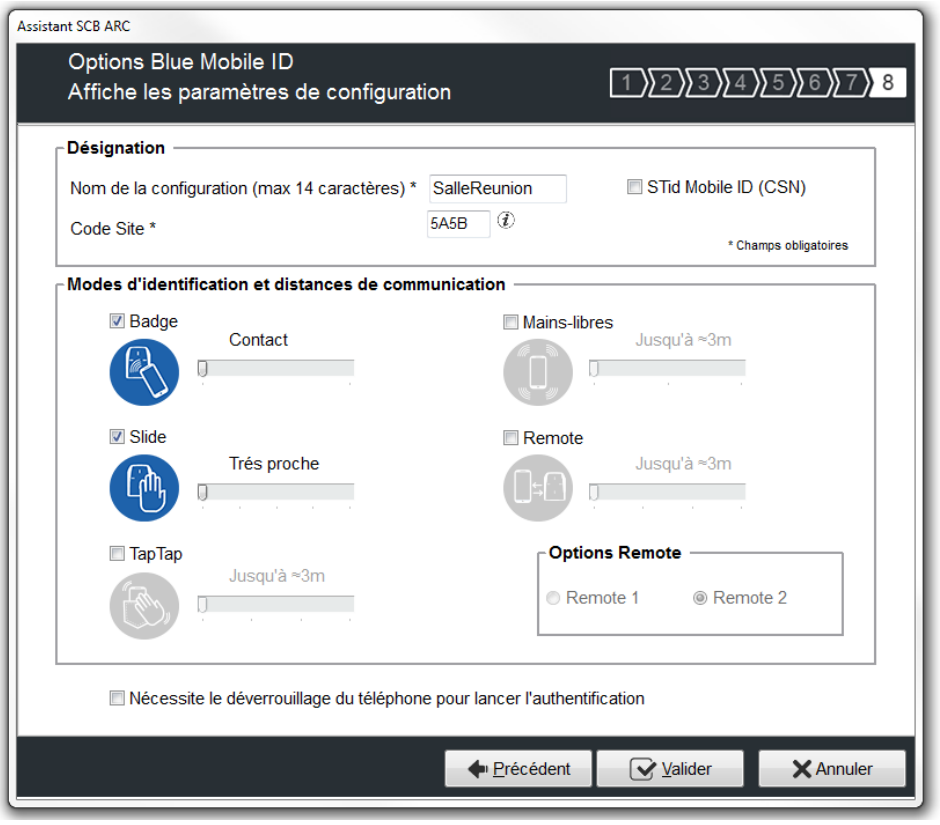
4. Paramètres SECard pour la création du badge de configuration Accueil



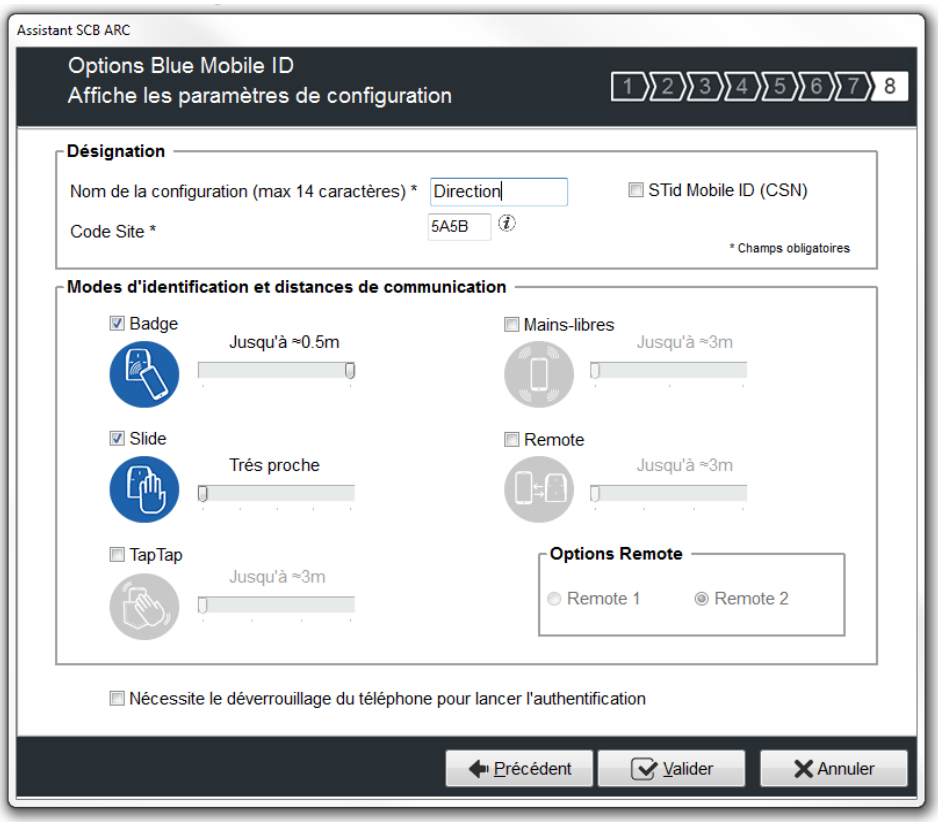
5. Paramètres SECard pour la création du badge de configuration Salle Serveur



6. Paramètres SECard pour la création du badge de configuration Salle de réunion



7. Paramètres SECard pour la création du badge de configuration Bureau Direction



8. Aperçu des badges de configuration dans l'Application STid Settings