TIL TECHNOLOGIES
by HIRSCH

Guide utilisateur des lecteurs évolution BLUE MOBILE ID

Référence du document : GU-10028-FR
Date de publication : 04/07/2025

Table des matières

Préface

1. Contexte d'utilisation de ce manuel

Les pastilles de couleur jaune en haut de chaque page signalent que ce document est un guide utilisateur.

Le partenaire ou installateur TIL TECHNOLOGIES configure l'installation chez le client.

2. Réserve de propriété

Les informations contenues dans ce document peuvent être modifiées sans avertissement.

Les informations citées dans ce document à titre d'exemple, ne peuvent en aucun cas engager la responsabilité de la société HIRSCH Secure SAS (ci-après nommée HIRSCH). Les sociétés, noms et données utilisés dans les exemples sont fictifs, sauf notification contraire.

TIL TECHNOLOGIES est une marque déposée de la société HIRSCH.

Toutes les marques citées sont des marques déposées de leurs propriétaires respectifs.

Envoyez vos commentaires, corrections et suggestions concernant ce guide à *documentation@hirschsecure.fr*

3. Glossaire

Les termes techniques utilisés dans ce guide sont expliqués ci-après.

Badge	Un badge permet d'identifier une personne sur un système de contrôle d'accès. Il comporte un identifiant (sécurisé ou pas) qui est détecté et traité par une tête de lecture physique. Cette opération peut nécessiter un contact direct (comme avec une carte à puce ou une bande magnétique) ou l'approche à distance (pour un badge NFC ou sans contact). Les badges les plus couramment utilisés sont de technologie MIFARE DESFIRE de type EV1, EV2 ou EV3.
Firmware	Microprogramme informatique stocké dans un équipement (*TILLYS*, modules, clavier TACTILLYS) qui définit son fonctionnement. Un firmware peut être mis à jour pour éviter de remplacer le matériel sur lequel il a été téléchargé.
GTB	Acronyme de Gestion Technique des Bâtiments.

	Système de pilotage, de contrôle, de supervision et d'optimisation des divers services comme l'éclairage, le chauffage ou la ventilation, présents dans les bâtiments tertiaires et industriels (immotique).
Identifiant	Élément permettant l'accès d'un identifié. Les identifiants peuvent faire appel à plusieurs technologies (porte clé, carte, plaque minéralogique, empreinte digitale, code numérique...) et divers types de lecteur pour les lire.
Identifié	Personne devant disposer d'un accès au site protégé par le système de contrôle d'accès. Un identifié peut être porteur d'un ou de plusieurs identifiants distincts. Les identifiés peuvent être : ● Des personnes travaillant en permanence sur le site (identifié de type "permanent"), ● Des intervenants externes au site (identifié ayant une durée de validité spécifique correspondant à la durée de son intervention), ● Des personnes ayant accès de façon temporaire au site (identifié de type "visiteur").
IP	Acronyme anglais d'Internet Protocol. Le protocole Internet permet aux équipements qui l'utilisent de communiquer entre eux par paquets, de type *TCP* ou *UDP*. Le protocole IP est transporté par des réseaux locaux filaires utilisant le protocole de connexion Ethernet. Les cartes ou interfaces réseau équipées de connecteurs de type *RJ45* y ont accès physiquement et y sont identifiées logiquement via leur adresse IP.
Lecteur	Équipement utilisé pour la détection d'un identifiant sur un système de contrôle d'accès. L'identifiant peut prendre différentes formes : badge, code clavier, empreinte biométrique, plaque minéralogique... Selon sa technologie, un lecteur peut être utilisé pour : ● Assurer la simple détection du support de l'identifiant, par exemple un lecteur de type "transparent" qui se limite à détecter la présence d'un badge. ● Assurer en plus la lecture d'un identifiant standard, par exemple un lecteur "simple" qui ne sait lire que le numéro de série d'un badge (identifiant *CSN*).

	• Assurer en plus la fonction de déchiffrement d'un identifiant sécurisé encodé dans un badge, par exemple un lecteur sécurisé dans lequel on enregistre la clé des badges.
Port	Point d'entrée à un service (service web, service DNS, service mail...) sur un équipement (PC, serveur...) connecté à un réseau. Les ports constituent des accès entrants ou sortants et ils permettent aux différents logiciels et/ou systèmes d'exploitation de communiquer entre eux.
Port réseau	Point d'entrée à un service (service web, service DNS, service mail...) sur un équipement (PC, serveur...) connecté à un réseau. Les ports constituent des accès entrants ou sortants et ils permettent aux différents logiciels et/ou systèmes d'exploitation de communiquer entre eux.
Port TCP	Point d'entrée TCP (Transmission Control Protocol). TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport au même titre que l'UDP, sauf qu'il travaille en mode connecté. Les données transmises sont donc vérifiées.
Port UDP	Point d'entrée UDP (User Datagram Protocol). Le protocole UDP est l'un des deux principaux protocoles utilisé sur les réseaux TCP/IP (avec TCP), que le réseau soit Ethernet ou sans fil. Contrairement au TCP, il ne permet pas à l'émetteur de vérifier si les données sont effectivement reçues en recevant un accusé de réception.
TILLYS	Automate *IP* programmable multifonction développé par TIL TECHNOLOGIES qui dispose des fonctionnalités de contrôle d'accès, de détection intrusion et de *GTB*. Grâce à 3 bus RS 485 (A, B et C), chaque TILLYS permet le raccordement de 8, 16 ou 24 lecteurs pour le contrôle d'accès. Elle constitue également une véritable centrale d'alarme. Voir aussi *UTL*.
UTL	Acronyme d'Unité de Traitement Local. Terme générique qui désigne un automate *IP* programmable et multifonction, utilisé dans le domaine du contrôle d'accès, de l'intrusion et de la GTB. C'est grâce à cet automate que vont être gérés par exemple, les accès des identifiés, les informations provenant des lecteurs ou des systèmes anti-intrusion, etc. L'UTL de TIL TECHNOLOGIES est la *TILLYS*, qui se décline en version V2, NG et CUBE.

Chapitre 1. Prérequis

1.1. Compatibilité smartphone

- ANDROID
- IPHONE

1.2. Compatibilité OS

- ANDROID version 5.0 ou supérieure.
- IOS version 9 ou supérieure.

1.3. Compatibilité BLUETOOTH

Bluetooth version 4.0 LE minimum.

1.4. Compatibilité lecteurs et kits de programmation

Lecteurs EVOLUTION data/clock et RS485 références :

- LEC05XF6xxx-xxx
- LEC05ST6xxx-xxx (avec biométrie)

Kit de programmation référence :

- PRG05XF06
- PRG05XF07 (avec biométrie)

1.5. Compatibilité logiciels

SECard version 3.4.0 ou supérieure.

STid Mobile ID de STid SAS version 1.0 ou supérieure.

STid Setting de STid SAS version 1.0 ou supérieure.

1.6. Compatibilité identifiants

- vCard STid Mobile ID.
- ISO14443 A & B, ISO18092 (NFC).
- MIFARE® Ultralight & Ultralight C, MIFARE Classic, MIFARE Plus, MIFARE DESFire EV1 & EV2, NFC, SMART MX, CPS3, Moneo, iCLASS, PicoPass.

Spécificités de fonctionnement et compatibilité:

- Le lecteur ne supporte la fonction NFC que **si** la lecture de badges ISO A / ISO B est désactivée.
- Si la lecture de badges ISO A / ISO B est activée **en même temps** que la fonction Bluetooth/NFC, seul un téléphone en bluetooth avec le NFC désactivé (ou des badges ISO A / ISO B) fonctionnera.
- Si les fonctions Bluetooth/NFC ainsi que ISO A / ISO B sont activées sur le lecteur, un téléphone badgeant avec le NFC activé ne remontera pas le bon code identifiant et l'**utilisateur ne sera pas reconnu**.

Chapitre 2. Principe de fonctionnement

2.1. Trois types de licences

- Mobile ID
  - Identifiant avec numéro unique fourni à l'installation de l'application
  - Un seul mode d'exploitation utilisable : proximité
  - Pas de crédit nécessaire.
- Mobile ID+
  - Identifiant avec numéro unique fourni à l'installation de l'application
  - Permet l'utilisation de 4 modes d'exploitations : proximité, slide, tap tap et longue distance.
  - Crédits nécessaires : référence TIL Technologies BAD05VT02.
- SECURE+
  - Identifiant avec ID Privé, sécurisation entièrement personnalisable
  - Permet l'utilisation de 4 modes d'exploitations et télécommandes : proximité, slide, tap tap et longue distance et 2 télécommandes
  - Crédits nécessaires : référence TIL Technologies BAD05VT01

2.2. Modes d'identification et distance de communication

Il existe plusieurs mode d'identification, pour chaque mode d'identification, la distance de communication est réglable.

La notion de distance en Bluetooth correspond à une zone autour du lecteur, pas seulement en façade.

Les distances de lecture dépendent de l'environnement, de la position du smartphone par rapport au lecteur.

Il est recommandé de faire des tests sur site pour valider les réglages.

- Proximité : Fonctionne en présentant le smartphone devant le lecteur (comme un badge)
  - Contact : le smartphone doit être en contact avec le lecteur
  - Jusqu'à 0.5m : le smartphone doit être dans une zone de 0.5m autour du lecteur.
- Slide : Fonctionne en effleurant le lecteur de la main sans présenter le téléphone au lecteur.
  - Très proche
  - Proche
  - Moyenne
  - Lointaine
  - Très lointaine

Le mode Slide est non disponible sur les lecteurs claviers EVOLUTION

- Tap Tap : Fonctionne en tapotant deux fois le téléphone dans la poche.
  - Jusqu'à 3m
  - Jusqu'à 5m
  - Jusqu'à 10m
  - Jusqu'à 15m
- Longue distance, mains-Libres : Fonctionne sans aucune action de l'utilisateur.
  - Jusqu'à 3m
  - Jusqu'à 5m
  - Jusqu'à 10m
- Remote : Fonctionne à distance. Le téléphone devient votre télécommande. On peut afficher jusqu'à deux boutons par badge virtuel.
  - Jusqu'à 3m
  - Jusqu'à 10m
  - Jusqu'à 15m
  - Jusqu'à 20m

Une seule télécommande par lecteur est configurable, l'ouverture sera commandée à distance soit avec la remonte 1 soit avec la remote 2.

Voir chapitre Configuration BLUE MOBILE ID étape 8.

2.3. Définitions

Badge de programmation SCB	Permet de configurer les lecteurs EVOLUTION (protocole de communication, mode de fonctionnement, clés pour le contrôle d'accès...). Ce badge peut être physique ou virtuel via l'application STid Settings.
Crédits	Pour encoder des badges utilisateurs virtuels dans le téléphone, il faut acheter des crédits d'encodage qui seront chargés dans l'encodeur. Le chargement des crédits se fait par l'intermédiaire du logiciel SECard.
STid Mobile ID	Cette application vous permet de ranger et organiser tous vos badges d'accès virtuels dans un seul portefeuille virtuel.
STid Settings	STid Settings est une application de paramétrage permettant de configurer les lecteurs EVOLUTION BLUE. Tous vos badges de programmation (SCB virtuels) sont centralisés et accessibles à partir de smartphones.
vCard	Identifiant Virtuel pour le contrôle d'accès disponible à partir de l'application STid Mobile ID pour Smartphone compatible avec les lecteurs EVOLUTION BLUE

Chapitre 3. Crédits

3.1. Commander des crédits

Pour commander les crédits nécessaires permettant l'encodage d'identifiants BLUETOOTH depuis votre encodeur, contacter TIL TECHNOLOGIES à l'adresse `<commandes@til-technologies.fr>` avec votre bon de commande et le fichier texte généré depuis l'encodeur. Il est possible de consulter le nombre de crédits disponibles depuis l'encodeur.

Pour générer le fichier texte qui doit être envoyé à TIL TECHNOLOGIES depuis votre encodeur, suivre les étapes ci-dessous. Ce code à générer (numéro RequestID) est indispensable à la génération des codes licence des crédits demandés.

1.. Se connecter à SECard.

2.. Aller dans *Paramètres > Crédit.*

3.. Sélectionner le nombre de crédits désirés et cliquer sur *Générer fichier texte*.

4.. Une fenêtre s'ouvre pour choisir l'emplacement et enregistrer le fichier.

3.2. Charger des crédits

Un fichier **.PSE** est nécessaire afin de charger les crédits via SECARD.

Après réception de la commande par TIL TECHNOLOGIES, vous recevrez les codes licence à charger dans votre encodeur. Procéder au chargement des crédits comme suit :

1.. Connecter l'encodeur qui a généré la demande de crédit.

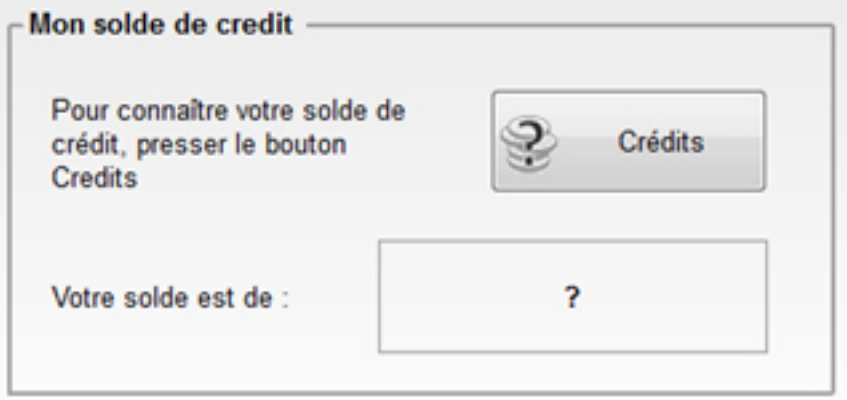
2.. Se connecter à SECard

3.. Aller dans *Paramètres > Crédit.*

4.. Entrer le code licence fourni.

5.. Cliquer sur *Chargement crédits*.

Mon solde de crédits permet de connaître le solde de crédits disponible dans l'encodeur.


Mon solde de credit
Pour connaître votre solde de crédit, presser le bouton Credits
Crédits
Votre solde est de :
?

Chapitre 4. Obtenir un identifiant virtuel vCard et changement de licence

4.1. Mode Mobile ID

Un identifiant unique gratuit est fourni à l'installation de l'application Mobile ID depuis l'AppStore ou le PlayStore.

4.2. Mode Mobile ID+

Un identifiant unique gratuit est fourni à l'installation de l'application Mobile ID depuis l'AppStore ou le PlayStore.

Pour bénéficier des avantages des modes d'authentification Slide, Tap Tap et longue distance, l'activation du mode Mobile ID+ est nécessaire.

Ceci décompte 1 crédit pour chaque smartphone passé en mode Mobile ID+.

Pour réaliser le passage d'un smartphone en mode Mobile ID+ réaliser les étapes suivantes :

1.. Connecter l'encodeur EVOLUTION

2.. Se connecter à SECard.

3.. Aller dans *Création badges > STid Mobile ID+.*

4.. Placer le smartphone sur l'encodeur EVOLUTION

5.. Clique sur *Promouvoir* (ceci décomptera 1 crédit)

4.3. Mode Secure+

Les identifiants privés doivent être encodés sur l'application Mobile ID via SECard et un encodeur EVOLUTION BLUE.

L'encodage d'identifiant privé décompte 5 crédits.

Le paramétrage de configuration des lecteurs doit être réalisé avant d'encoder les identifiants privés.

Veuillez vous référer au chapitre Configuration BLUE MODILE ID

Ne jamais modifier le code site une fois les identifiants privés encodés, cela impliquerait de ré-encoder tous les identifiants avec un décompte de 5 crédits par smartphone.

Chapitre 5. Configuration BLUE MOBILE ID

5.1. Paramétrages de SECARD

1.. Connecter l'encodeur STid ARC-W35-G/BT1-5AA à un port du PC.

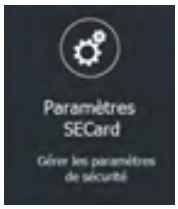
2.. Lancer le logiciel SECard

SECARD v 3.4.0 ou supérieur est nécessaire.

3.. Lors de la première utilisation, le logiciel affiche une fenêtre demandant de renseigner le numéro d'identification sur 32 caractères se trouvant au dos de l'encodeur. Après avoir enregistré le numéro, le logiciel ne réitérera plus sa demande.

4.. Dans paramètres SECard sélectionner le port COM sur lequel l'encodeur a été connecté.

Si vous ne connaissez pas le numéro, cliquer sur le point d'interrogation.



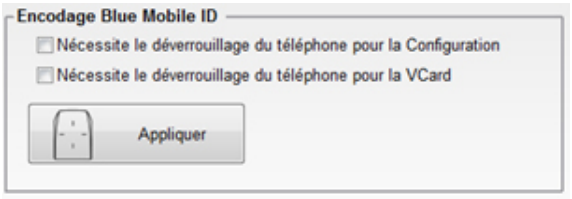
5.. Options déverrouillage du smartphone

Options de sécurité pour l'authentification d'une vCart sur un lecteur ou pour la configuration d'un lecteur EVOLUTION.

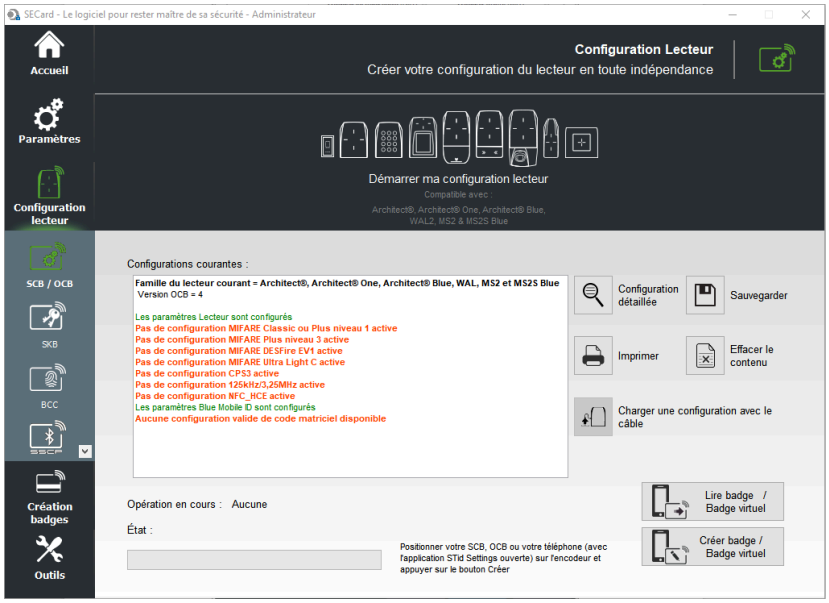
- Si cochée : le smartphone doit être déverrouillé pour s'authentifier ou configurer un lecteur.

Le déverrouillage du lecteur exige un code PIN, ou autre option de déverrouillage relative au modèle de smartphone.

- Si non cochée : le déverrouillage du smartphone n'est pas requis pour s'authentifier avec le lecteur.

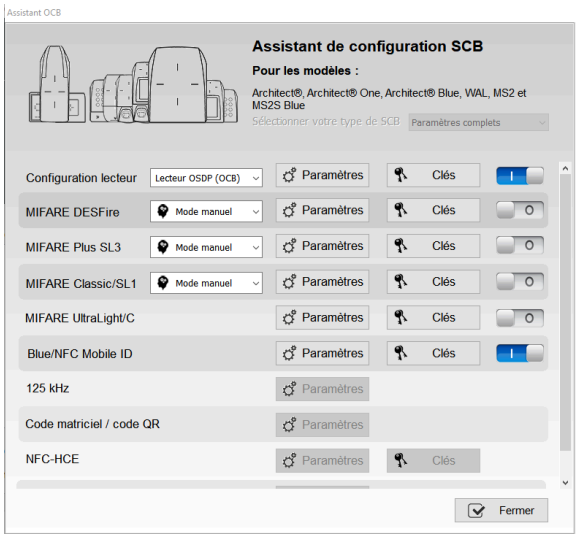
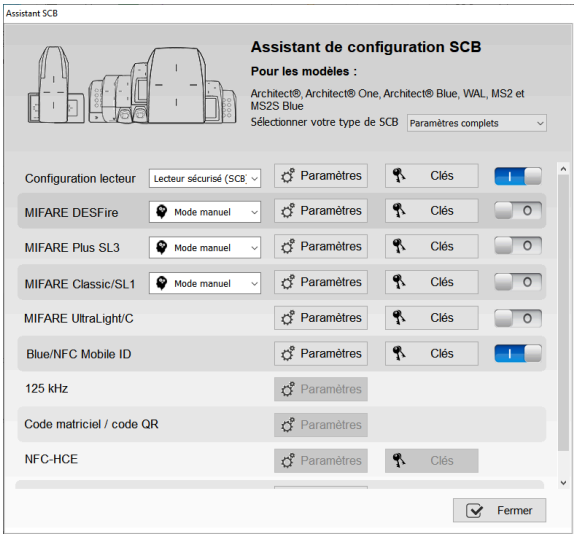


5.2. Sélectionner l'assistant de configuration SCB/OCB



5.3. Configuration du lecteur

Dans l'assistant SCB/OCB, Cliquer sur **Démarrer ma configuration lecteur**, choisir **Lecteur OSDP** ou **Lecteur SCB** :

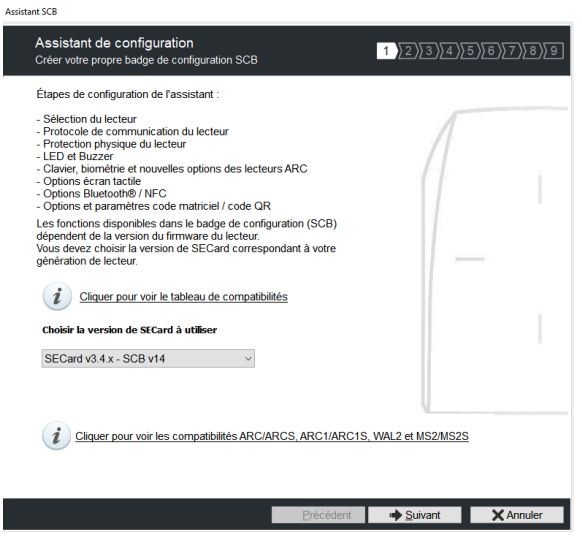
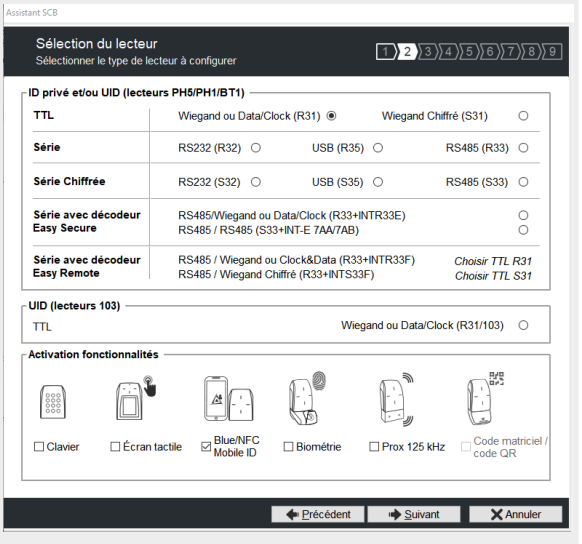
Configuration OSDP (OCB)	Configuration Sécurisée (SCB)
	

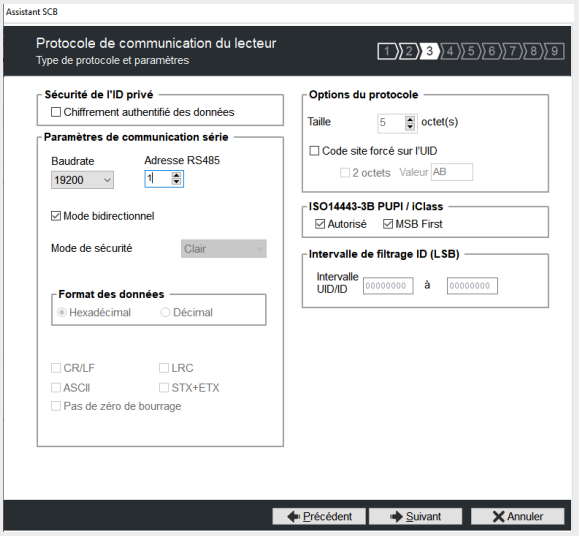
Lecteur sécurisé (SCB)

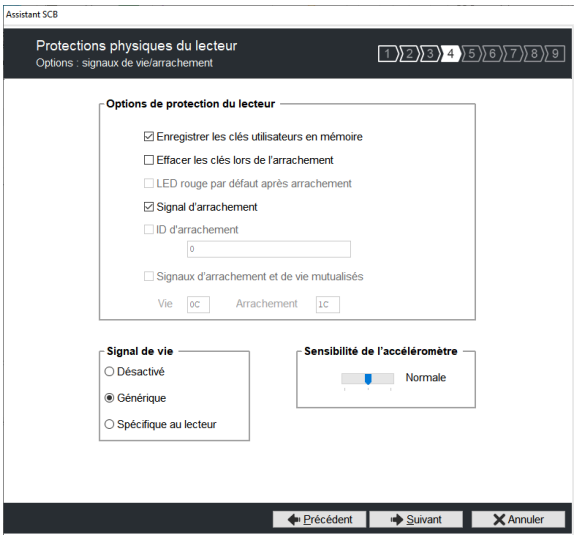
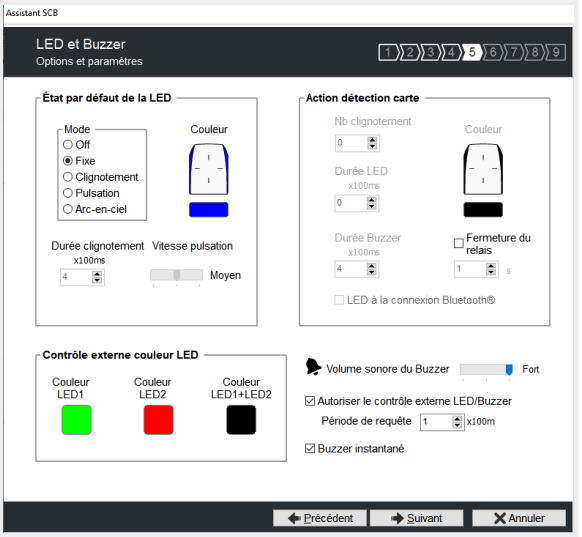
L'assistant de configuration se lance:

Suivre les 8 étapes de l'assistant.

Ci-dessous, uniquement les étapes et paramètres obligatoires (selon le type de lecteur) sont détaillés:

Assistant SCB	Assistant SCB
• Dans "Sélectionner la version de SECARD à utiliser", sélectionner la version de SECARD v3.4 x.	
• Activation des fonctions externes. Cocher ou décocher les options nécessaires pour les configurer: clavier, biométrie, écran tactile, Blue Mobile ID. • Pour lecteurs R31, cocher l'option **Wiegand ou Data/Clock (R31)** • Pour lecteurs R33 (Référence produit "-xb5t"), cocher l'option **RS 485 (R33)**	

Assistant SCB	Assistant SCB
OptionWiegand ou Data/Clock (R31) • Choisir le protocole **Clock&Data 40 bits - ISO 2B**	
OptionRS 485 (R33) • Dans **Paramètres de communication série**, cocher **Mode bidirectionnel** • **Baudrate** 19200 • **Adresse RS485** 1	

Assistant SCB	Assistant SCB
● Dans **Signal de vie**, choisir **Générique**	
OptionRS 485 (R33) ● Cocher **Autoriser le contrôle externe** ● **Période de requête** 1 ● Cocher **Buzzer instantané** ● Dans **Etat par défaut de la Led**, **Mode**, cocher **Fixe** **OptionWiegand ou Data/Clock (R31)** ● Passer à l'étape suivante	

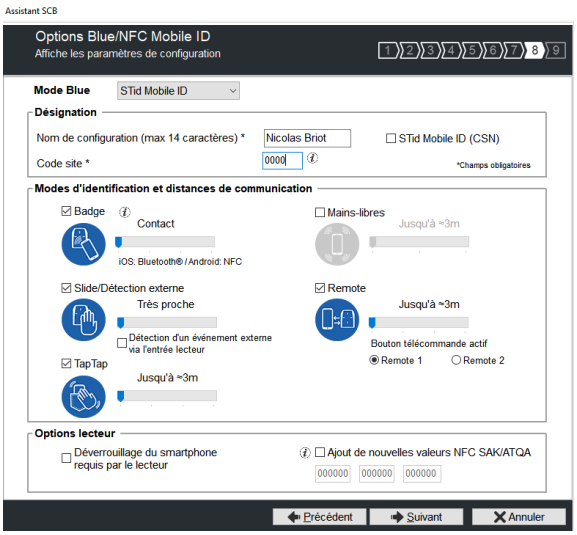
Assistant SCB

- Pour le mode Mobile ID+, configurer les modes d'identification à utiliser (proximité, slide, tap tap, mains-libres) et les distances de communication, selon votre installation.
- Pour le mode Secure+, indiquer un *Nom de configuration* et un *Code Site*

Ne jamais modifier le code site une fois les identifiants privés encodés, cela impliquerait de ré-encoder tous les identifiants avec un décompte de 5 crédits par smartphone.

Si le mode « Mains-libres » est activé, du fait de la technologie Bluetooth il prendra la main sur les autres modes.

Assistant SCB



Lecteur OSDP (OCB)

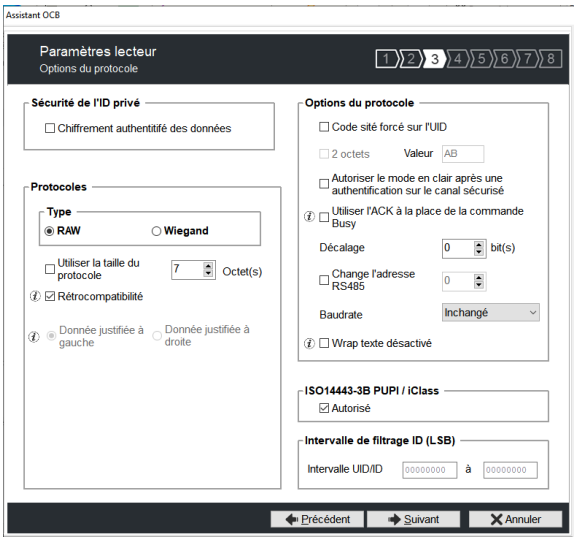
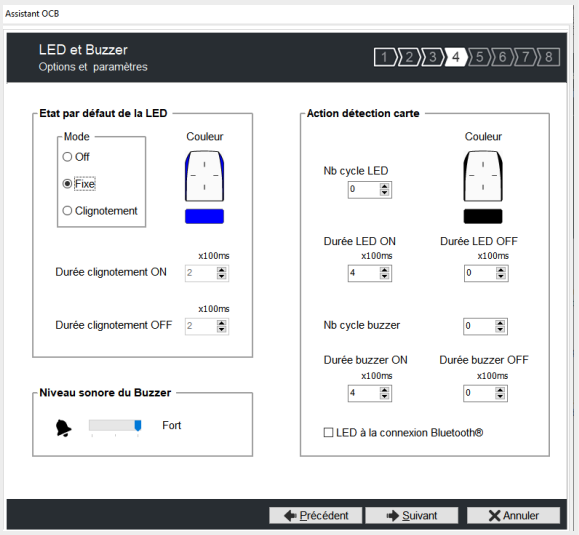
Pour un lecteur OSDP en configuration Usine, Cliquer sur **Clés**puis cocher **Utiliser une clé de transport**.

L'assistant de configuration se lance

Suivre les 8 étapes de l'assistant.

Ci-dessous, uniquement les étapes et paramètres obligatoires (selon le type de lecteur) sont détaillés:

Assistant OCB	Assistant OCB
• Dans **Sélectionner la version de SECARD à utiliser**, sélectionner la version de SECARD v3.4 x.	
• Activation des fonctions externes. Cocher ou décocher les options nécessaires pour les configurer: clavier, biométrie, écran tactile, Blue Mobile ID.	

Assistant OCB	Assistant OCB
• Dans **Protocoles**, **Type**, cocher **RAW**	
• Dans **Etat par défaut de la Led**, **Mode**, cocher **Fixe**	

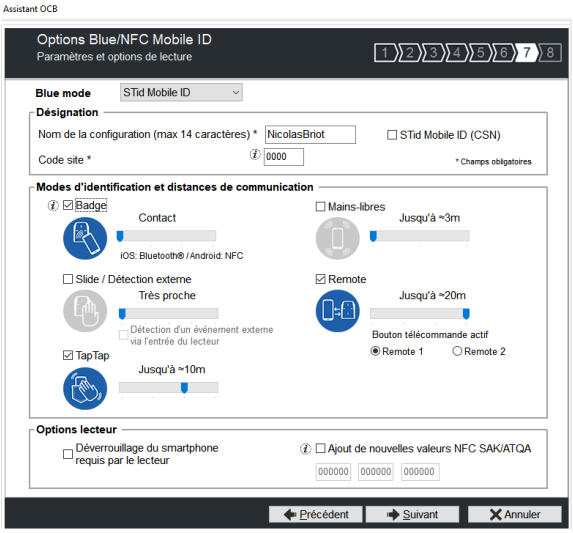
Assistant OCB

- Pour le mode Mobile ID+, configurer les modes d'identification à utiliser (proximité, slide, tap tap, mains-libres) et les distances de communication, selon votre installation.
- Pour le mode Secure+, indiquer un *Nom de configuration* et un *Code Site*

Ne jamais modifier le code site une fois les identifiants privés encodés, cela impliquerait de ré-encoder tous les identifiants avec un décompte de 5 crédits par smartphone.

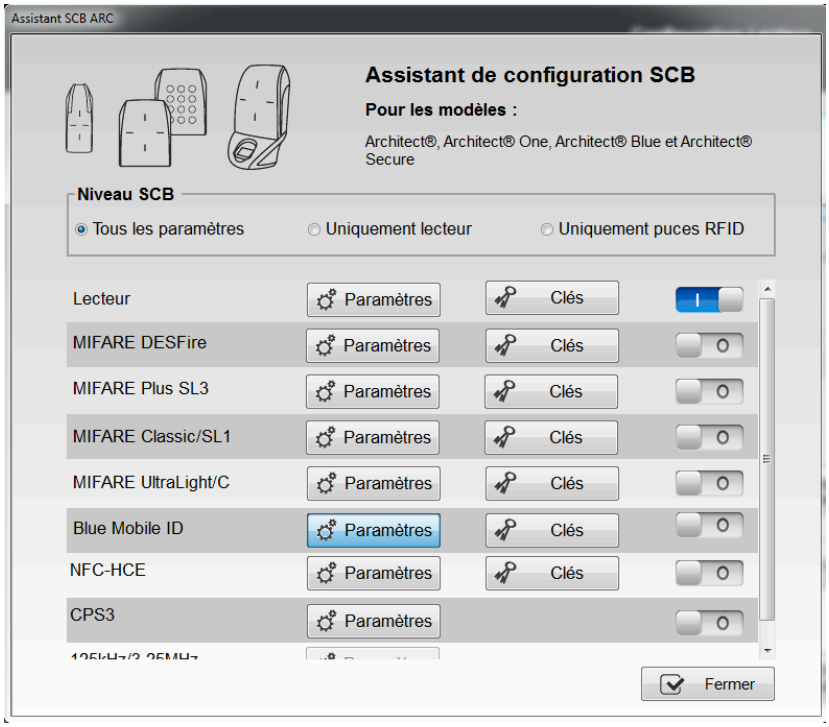
Si le mode « Mains-libres » est activé, du fait de la technologie Bluetooth il prendra la main sur les autres modes.

Assistant OCB



5.4. Blue Mobile ID : paramètres de sécurité (mode Secure+ uniquement)

Dans l'assistant de configuration SCB, accéder aux paramètres pour Blue Mobile ID :



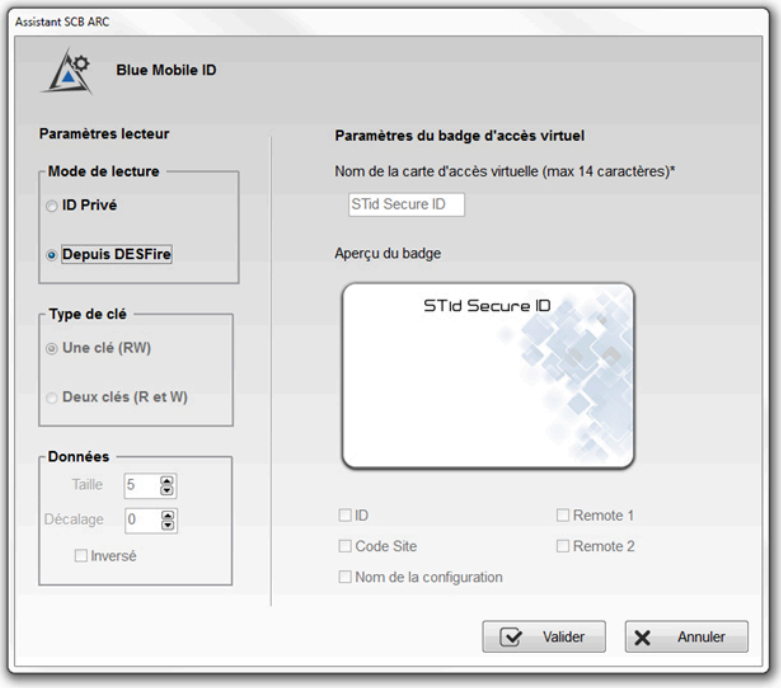
Indiquer les paramètres suivants :

- Mode de lecteur : *ID Privé* ou *Depuis DESFire*

  Depuis DESFire : Paramètre à utiliser si une configuration de clé ID Privé est déjà configuré pour le mode Mifare DESFire.

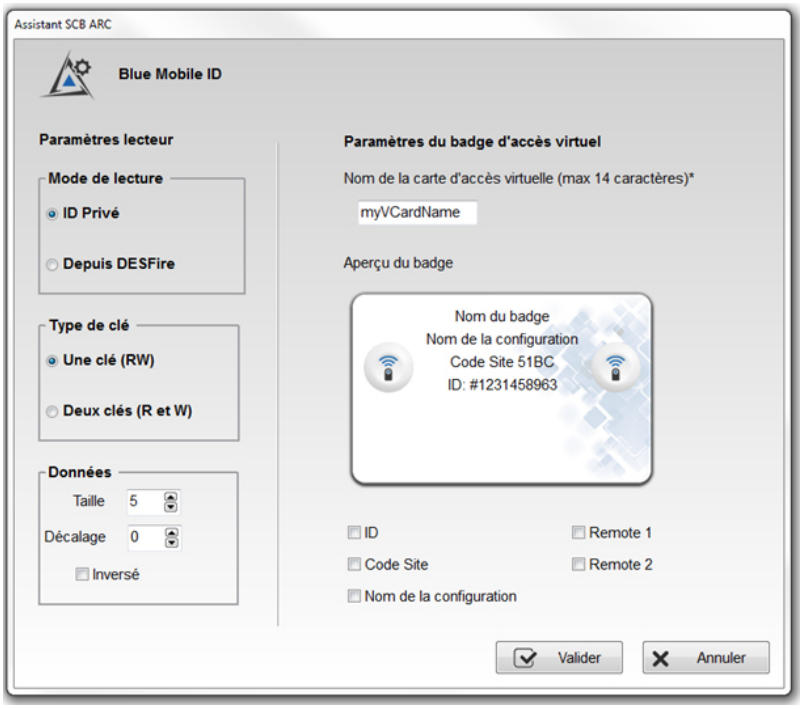
  Dans ce cas une configuration DESFire doit être active sinon un message d'erreur apparaîtra.

  Dans ce mode, tous les paramètres BlueMobile ID sont automatiquement déterminés et hérités des paramètres définis pour la DESFire. Les paramètres lecteurs sont donc modifiés et passe sur la configuration SameAsDESFire. Cliquer sur le bouton "Valider" pour terminer la configuration.



ID Privé : Paramètre à utiliser si aucune configuration clé Mifare DESFire n'est réalisée.

Dans ce mode vous pourrez dans la partie Mifare DESFire récupérer les clés de lecture et d'écriture configuré pour le Modile ID.



Lecteur configuré en lecture de l'identifiant privé uniquement :

Type de clé	Description
Une clé (RW)	Utilise une clé unique pour la lecture et l'écriture.
Deux clés (R et W)	Utilise une clé pour la lecture et une clé différente pour l'écriture

Data	Description
Taille	Détermine la longueur de l'identifiant.
Décalage	Définie un décalage à partir du premier octet pour la lecture des données.
Inversé	Si la case est cochée l'identifiant est lu Least Significant Byte First (LSB). Si la case n'est pas cochée, l'identifiant est lu Most Significant Byte First (MSB).

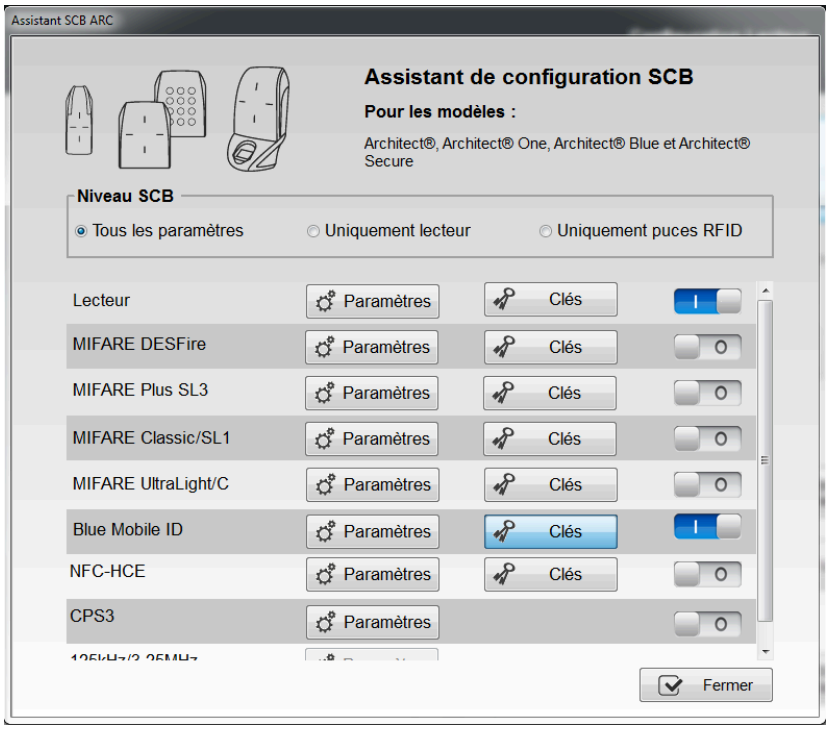
- Paramètres de l'identifiant d'accès virtuel :

  Les paramètres suivants permettent de personnaliser les informations de la vCard affichées dans l'application Mobile ID.

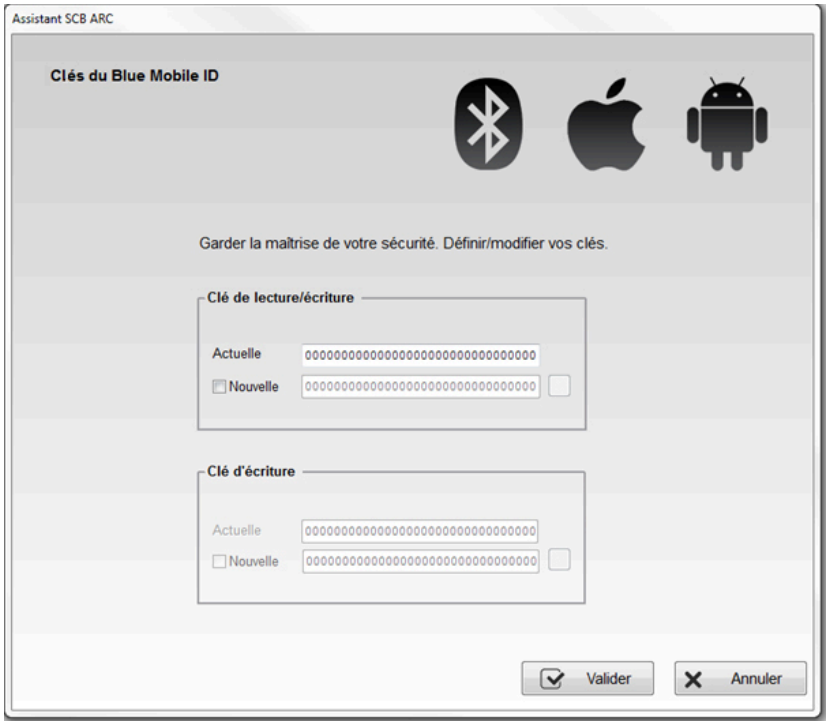
  - Nom de la carte d'accès : Nom qui apparaîtra sur le badge virtuel à l'écran du smartphone. Choisir un nom significatif permettant à l'utilisateur d'identifier rapidement le badge virtuel à utiliser.
  - ID
  - Code site
  - Remote 1 : télécommande 1
  - Remote 2 : télécommande 2

5.5. Blue Mobile ID : clés

Dans l'assistant de configuration SCB, accéder aux clés pour Blue Mobile ID :



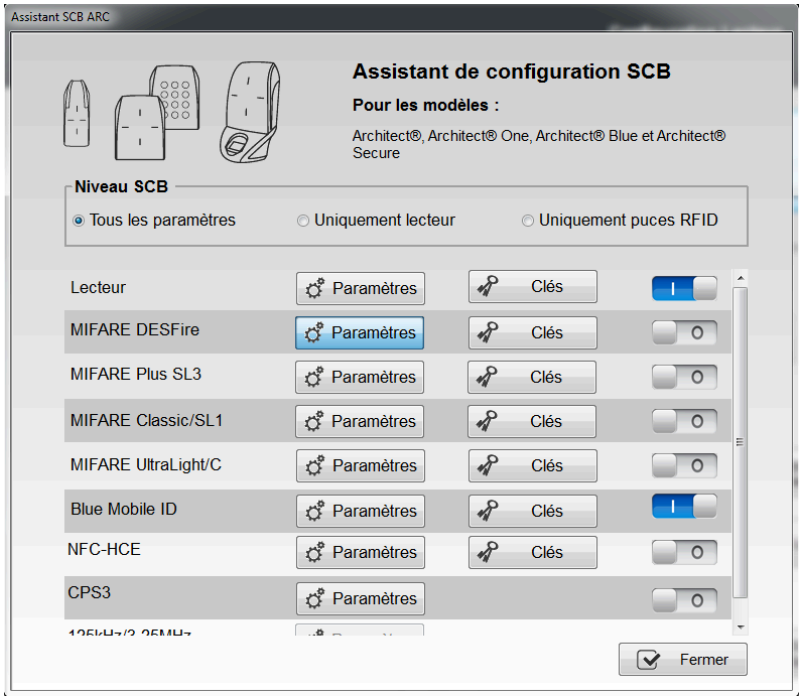
Cette interface permet de définir les clés de sécurité utilisées pour les données Blue. Les clés par défaut sont 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.



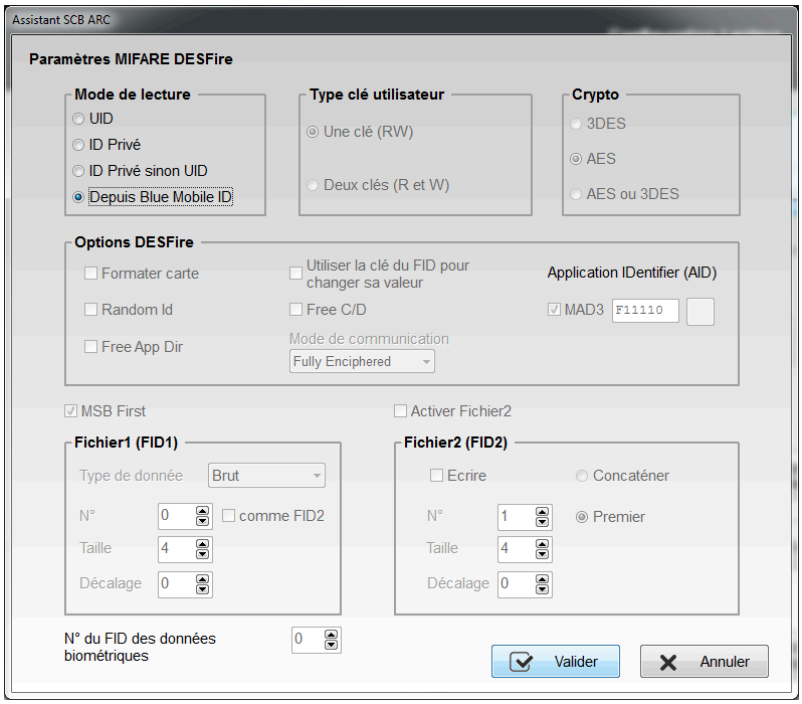
5.6. Configuration DESFire avec clés de lecture et écriture Mobile ID (mode Secure+ uniquement)

Dans le cas où vous souhaitez utiliser le même identifiant en Virtual Access Card et sur un support physique DESFire, suivre les étapes ci-dessous :

1.. Dans l'assistant SCB, accéder aux paramètres pour MIFARE DESFire :



2.. En sélectionnant le mode de lecture “Depuis Blue Mobile ID” tous les paramètres et les clés DESFire sont hérités de la configuration Blue Mobile ID et apparaissent donc grisés dans l’assistant.



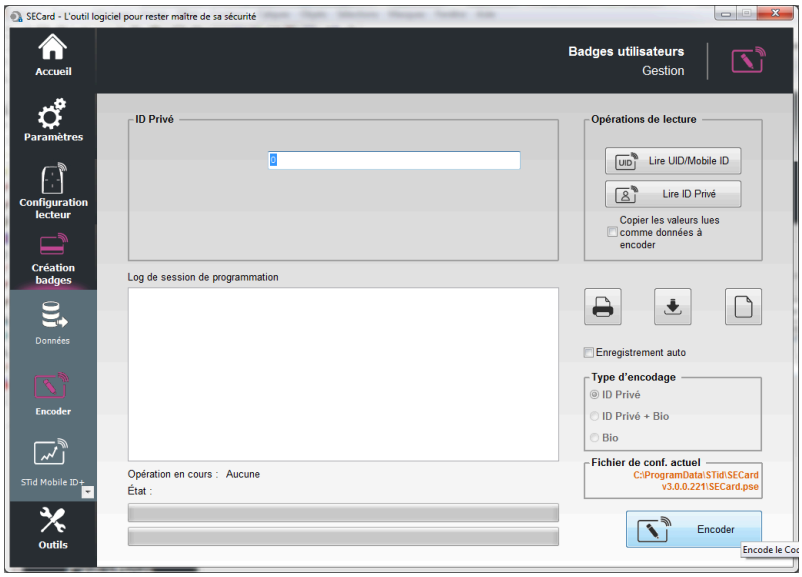
Dans le cas d'une configuration Blue en mode "Deux Clés" la clé d'écriture sera la clé numéro 1.

5.7. Encodage de l'identifiant privé

Avec identifiants dématérialisés SECURE+, il est nécessaire d'encoder l'identifiant privé.

L'encodage de l'identifiant privé nécessite l'application STid MOBILE ID.

1.. Placer le smartphone sur l'encodeur et cliquer sur Encoder.



2.. Une confirmation de la quantité de crédits consommés sera affichée. Cliquer sur "Oui". L'opération d'encodage s'affiche sur le logiciel SECARD et aussi dans l'application STid MOBILE ID.

3.. En cas d'utilisation d'un badge MIFARE® DESFire® EV1, placer le badge sur l'encodeur et cliquer sur Encoder.

Le paramétrage de configuration des lecteurs doit être réalisé avant d'encoder les identifiants privés.

Ne jamais modifier le code site une fois les identifiants privés encodés, cela impliquerait de ré-encoder tous les identifiants avec un décompte de 5 crédits par smartphone.

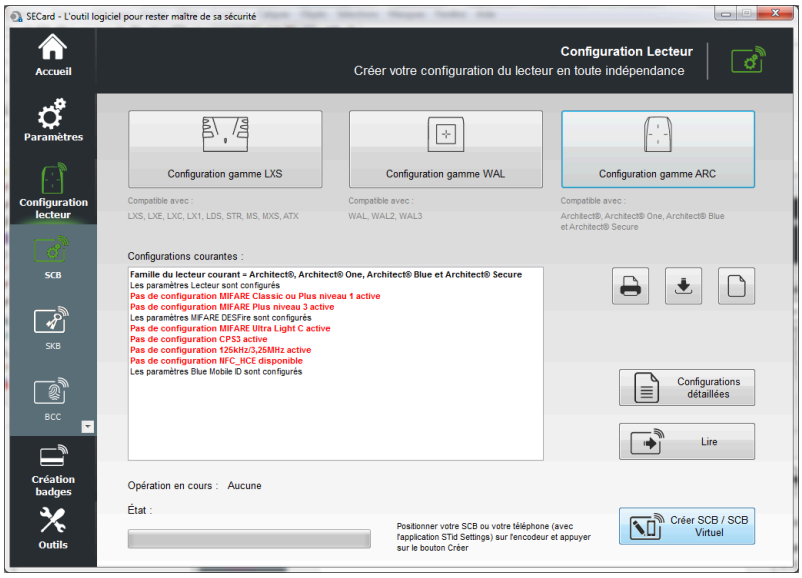
5.8. Création du badge de configuration virtuel pour lecteur EVOLUTION BLUE

1.. Installer l'application STiD Settings.

2.. Ouvrir l'application STid Settings sur le smartphone.

3.. Poser le smartphone sur l'encodeur et cliquer sur Créer SCB / SCB virtuel.

La création de badge SCB virtuel ne décompte pas de crédit.



4.. La création terminée vous pouvez voir le badge à l'écran et le message dans SECard.

5.. Vous pouvez créer un badge SCB physique en utilisant une MIFARE® DESFire® EV1 4Ko minimum. Poser le badge sur l'encodeur et cliquer sur Créer SCB / SCB virtuel.

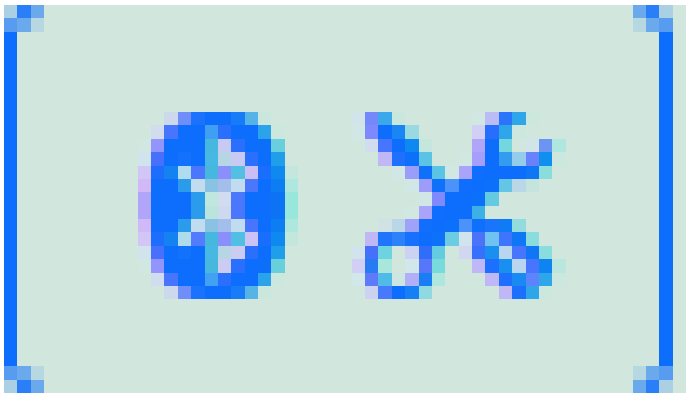
5.9. Activation du mode configuration bluetooth pour lecteurs SSCP

A partir de la version 5.9 de la TILLYS, il est nécessaire d'effectuer une procédure spécifique pour activer le mode configuration des lecteurs **Evolution transparents Bluetooth SSCP** .

Il est nécessaire au préalable d'activer le bluetooth dans la configuration du module de contrôle d'accès depuis la page **Reader Technology**.

Suivre la procédure suivante pour configurer un lecteur bluetooth EVOLUTION SSCP avec un badge de configuration :

1. Se rendre dans la page **Maintenance > Reader diagnostic**
2. Localiser le lecteur Bluetooth à configurer.

3. Cliquer sur l'icône  associée et vérifier l'apparition du bandeau de conifirmation dans la partie supérieure de la fenêtre.
4. Passer le badge de configuration devant le lecteur dans un intervalle de temps inférieur à 5 min.

Lors de l'activation du mode configuration bluetooth pour un lecteur, ce dernier ne peut êtte utilisé pour exécuter des opérations de contrôle d'accès pendant 5 minutes ou jusqu'à la présentation d'un badge de configuration.

Chapitre 6. Annexe - Encodage de vCard

6.1. Méthodes d'encodage des badges virtuels

Choisir une des**deux méthodes** d'encodage de Vcards (badges virtuels) avec un smartphone :

- Encodage des Vcards physiquement**avec l'encodeur** STID Bluetooth et un smartphone.

  Cette méthode permet la création d'un badge virtuel avec un encodeur physique de chez STID via l'application SECARD en mode opérateur.

  La création d'un badge à la volée permet de donner rapidement une Vcard à l'utilisateur.

  La révocation identifiants et la réutilisation des crédits n'est pas possible avec cette méthode.

- Encodage des Vcards **avec le cloud** de STID (sans encodeur STID).

  Cette méthode permet la création de badges virtuels encodés avec un fichier .PSE pré-chargé, avec envoi d'e-mail vers l'utilisateur de la Vcard encodée.

  La gestion de la population de Vcards est simplifiée: Il est possible de créer, révoquer, modifier des Vcards ainsi que d'importer/exporter le fichier.

  Les identifiants "5 crédits" crées par le cloud peuvent être révoqués : En cas de révocation de ce type d'identifiant, le compte client est ensuite ré-crédité, permettant la réutilisation de ces crédits.

  Prérequis obligatoires pour l'utilisation de cette méthode :

  - Un compte administrateur doit être crée au préalable et accessible depuis le smartphone.
  - Le smartphone doit avoir accès aux données mobiles.
  - Le smartphone doit être compatible avec STID MOBILE ID.

6.2. Encodage de vCards avec l'encodeur STID Bluetooth et un smartphone

Un fichier **.PSE** est nécessaire afin de charger les crédits via SECARD.

Après réception de la commande par TIL TECHNOLOGIES, vous recevrez les codes licence à charger dans votre encodeur. Procéder au **chargement des crédits** comme suit :

1.. Connecter l'encodeur qui a généré la demande de crédit.

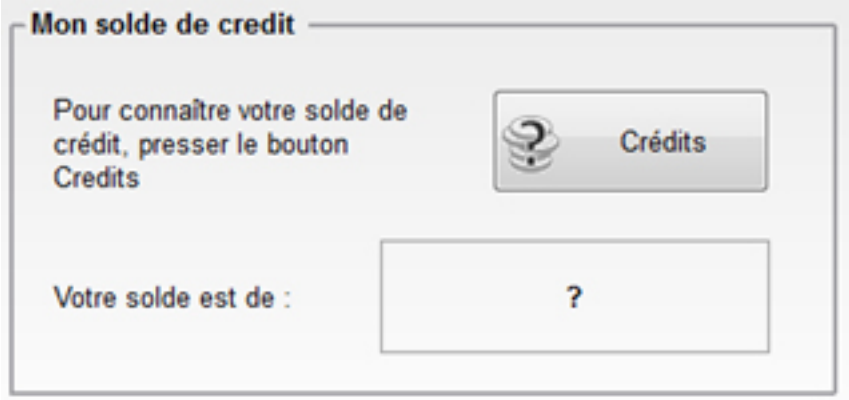
2.. Se connecter à SECard

3.. Aller dans *Paramètres > Crédit.*

4.. Entrer le code licence fourni.

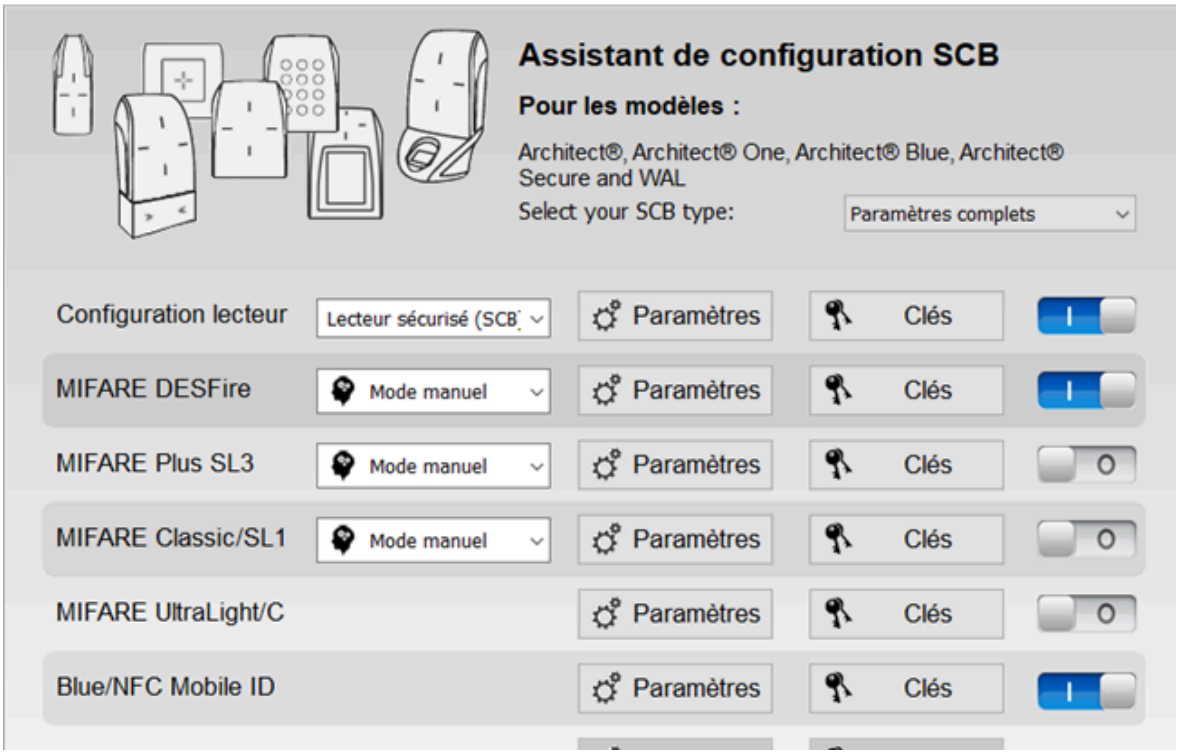
5.. Cliquer sur *Chargement crédits*.

Mon solde de crédits permet de connaître le solde de crédits disponible dans l'encodeur.



Dans l'**Assistant de configuration SCB**, vérifier que les **clés** pour MIFARE DESFire et Blue/NFC Mobile ID sont les mêmes.

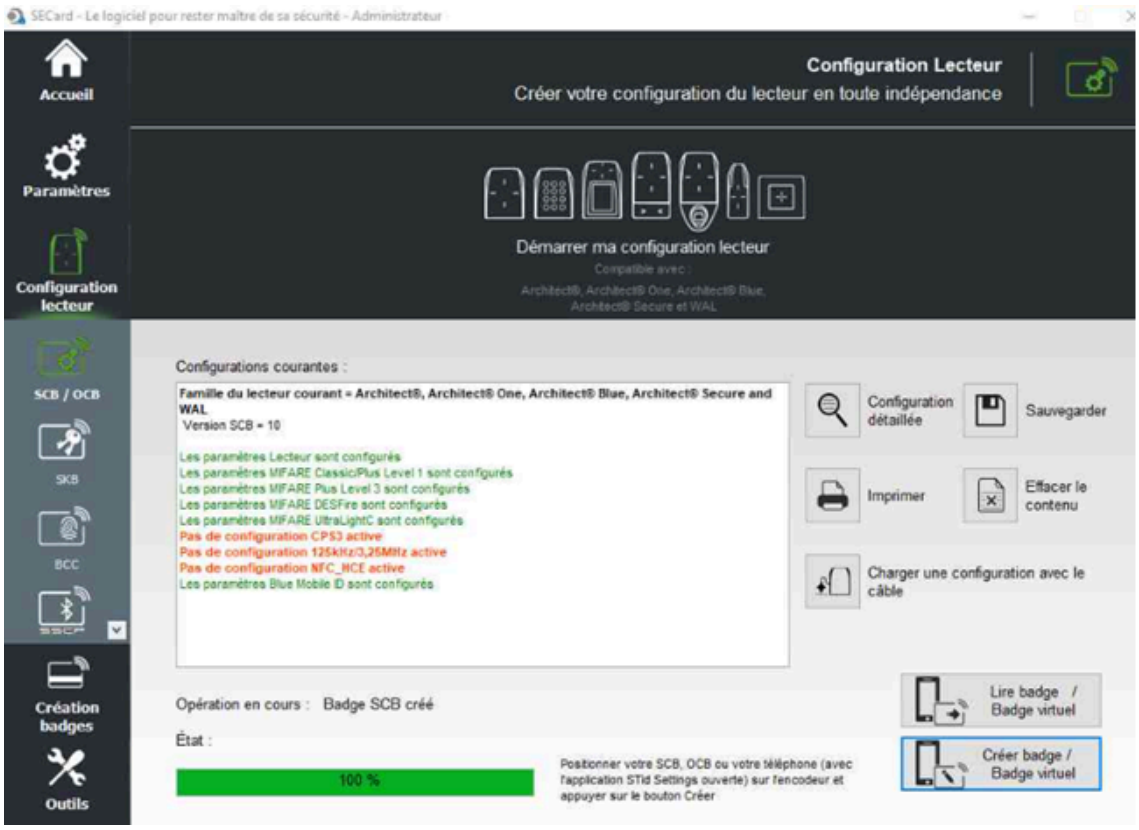
Assistant SCB



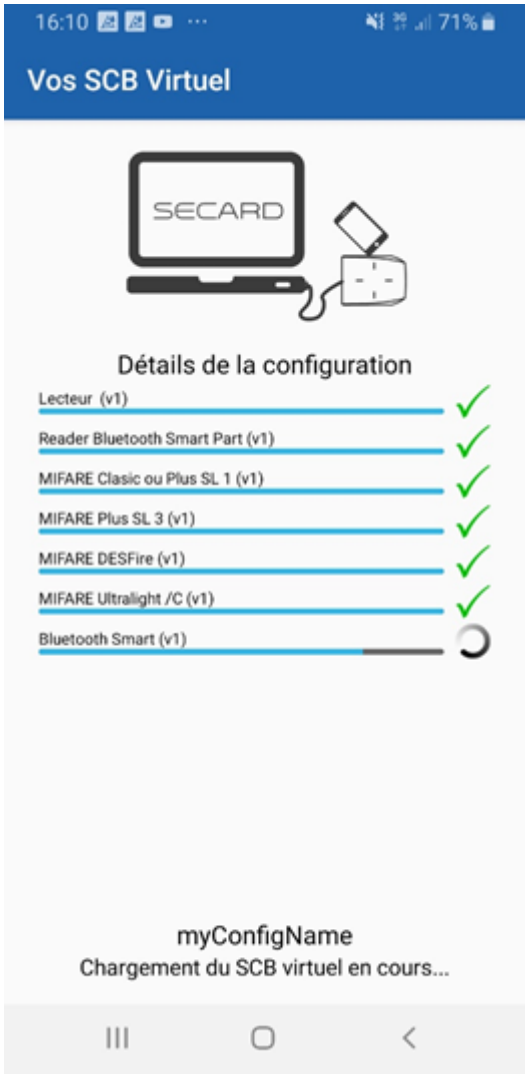
Récupérer l'application **STiD Settings** et l'installer dans le smartphone. L'activation du Bluetooth dans le smartphone est nécessaire.

Configurer le badge SCB :

1. Dans le logiciel SECARD, la vue suivante doit être affichée.


SECard - Le logiciel pour rester maître de sa sécurité - Administrateur
Accueil
Paramètres
Configuration lecteur
SCB / OCB
SKB
BCC
Création badges
Outils
Configuration Lecteur
Créer votre configuration du lecteur en toute indépendance
Démarrer ma configuration lecteur
Compatible avec :
Architect®, Architect® One, Architect® Blue, Architect® Secure et WAL
Configurations courantes :
Famille du lecteur courant = Architect®, Architect® One, Architect® Blue, Architect® Secure and WAL
Version SCB = 10
Les paramètres Lecteur sont configurés
Les paramètres MIFARE Classic/Plus Level 1 sont configurés
Les paramètres MIFARE Plus Level 3 sont configurés
Les paramètres MIFARE DESFire sont configurés
Les paramètres MIFARE UltraLightC sont configurés
Pas de configuration CPS3 active
Pas de configuration 125kHz/3,25MHz active
Pas de configuration NFC_NCE active
Les paramètres Blue Mobile ID sont configurés
Configuration détaillée
Sauvegarder
Imprimer
Effacer le contenu
Charger une configuration avec le câble
Opération en cours : Badge SCB créé
État :
100 %
Positionner votre SCB, OCB ou votre téléphone (avec l'application STid Settings ouverte) sur l'encodeur et appuyer sur le bouton Créer
Lire badge / Badge virtuel
Créer badge / Badge virtuel

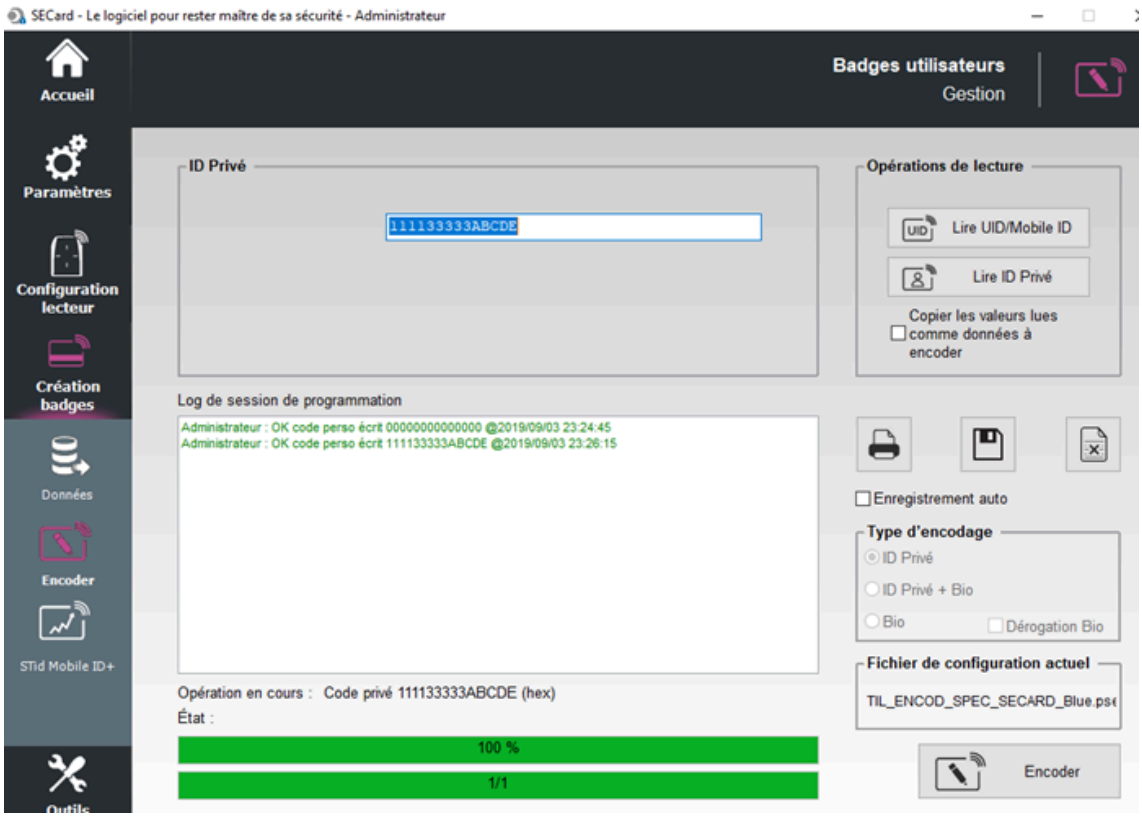
2. Dans l'application smartphone, la vue suivante doit être affichée.



3. Une fois le PSE chargé à travers l'encodeur Bluetooth sur le smartphone, la vue suivante doit être affichée.

4. Transférer les données sur le lecteur Bluetooth :
   - Présenter le smartphone sur le lecteur à programmer.
   - Sélectionner le SCB et appuyer sur "Configure".
   - La vue suivante doit s'afficher :

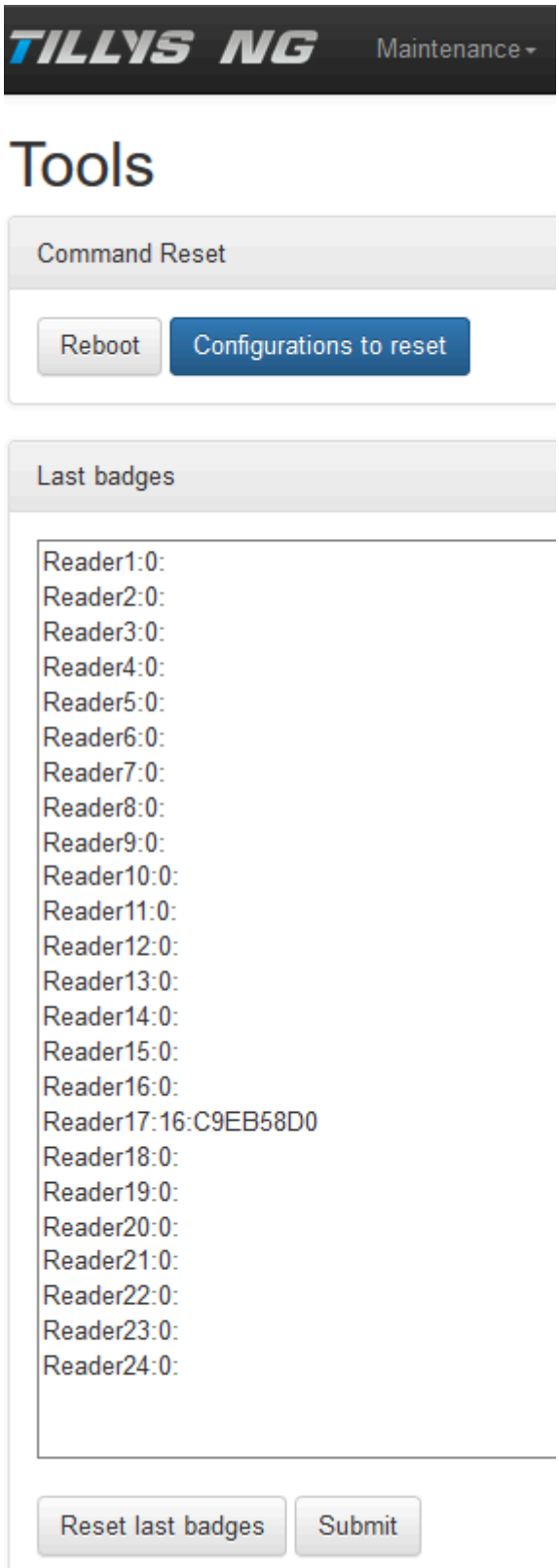
5. Lancer l'application SECARD pour encoder le smartphone sur le lecteur :


SECard - Le logiciel pour rester maître de sa sécurité - Administrateur
Accueil
Paramètres
Configuration lecteur
Création badges
Données
Encoder
STid Mobile ID+
Outils
Badges utilisateurs
Gestion
ID Privé
111133333ABCDE
Opérations de lecture
Lire UID/Mobile ID
Lire ID Privé
Copier les valeurs lues comme données à encoder
Log de session de programmation
Administrateur : OK code perso écrit 00000000000000 @2019/09/03 23:24:45
Administrateur : OK code perso écrit 111133333ABCDE @2019/09/03 23:26:15
Enregistrement auto
Type d'encodage
ID Privé
ID Privé + Bio
Bio
Dérogation Bio
Fichier de configuration actuel
TIL_ENCOD_SPEC_SECARD_Blue.pse
Opération en cours : Code privé 111133333ABCDE (hex)
État :
100 %
1/1
Encoder

6. Lancer l'application STID MOBILE ID et présenter son smartphone sur le lecteur.

   (L'application STID MOBILE ID contient les crédits virtuels chargés).

7. Au niveau de la TILLYS NG, le code correspondant au badge doit être indiqué. (Dans l'exemple ci-dessous, hexa car pilote 3 sélectionné - reader 17).

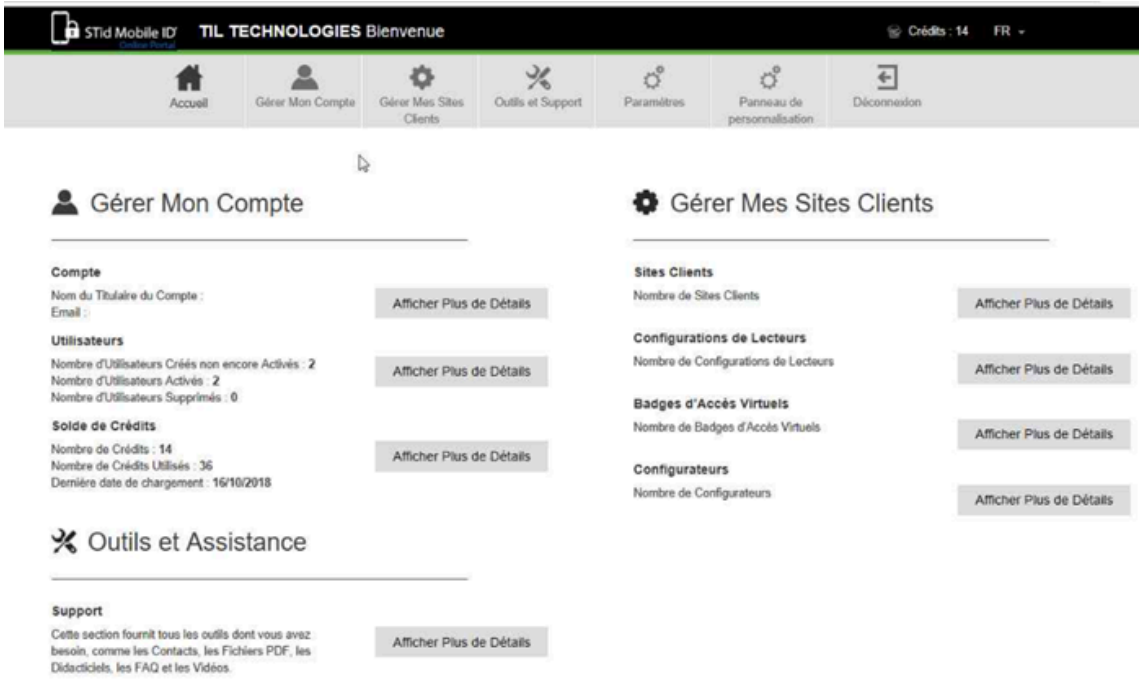

TILLYS NG
Maintenance
Tools
Command Reset
Reboot
Configurations to reset
Last badges
Reader1:0:
Reader2:0:
Reader3:0:
Reader4:0:
Reader5:0:
Reader6:0:
Reader7:0:
Reader8:0:
Reader9:0:
Reader10:0:
Reader11:0:
Reader12:0:
Reader13:0:
Reader14:0:
Reader15:0:
Reader16:0:
Reader17:16:C9EB58D0
Reader18:0:
Reader19:0:
Reader20:0:
Reader21:0:
Reader22:0:
Reader23:0:
Reader24:0:
Reset last badges
Submit

6.3. Encodage de vCards avec le cloud STID et un smartphone

Un fichier **.PSE** est nécessaire afin de charger les crédits via SECARD (voir étape 2).

1. Un **compte administrateur** est nécessaire afin d'utiliser cette méthode.

   Lors que le compte est activé et l'utilisateur Administrateur identifié, le compte doit s'afficher comme dans l'exemple :



2. Dans la section **Configuration des lecteurs**, importer le fichier PSE (bouton "Importer un fichier PSE") :

3. Dans la section **Gérer mes sites clients**, aller dans **Badges d'Accès Virtuels** et cliquer sur **Afficher plus de détails** :

Ajouter permet de créer un nouvel utilisateur de VCard.
Renseigner la fiche utilisateur. L'adresse e-mail est obligatoire.
Lors que l'utilisateur est généré et la Vcard est correctement envoyée, le statut "Badge virtuel envoyé avec succès" est afiché pour l'utilisateur concerné.

4. Avec le smartphone, vérifier que l'application STID MOBILE ID est installée. En cas contraire, faire le nécessaire.
5. Avec le smartphone (avec accès aux données activé), aller dans la boîte e-mail pour ouvrir l'e-mail envoyé dans l'étape 3 (Message de **STID MOBILE ID : Download your STID mobile Virtual Access Card**...).
6. Choisir le type de smartphone (Android / iPhone) en cliquant sur le lien approprié dans le message. Ouvrir le lien avec l'application STID MOBILE ID.
7. Un badge prêt à être utilisé est affiché.